Dinesh Khattar
Neha Agrawal

Group Theory

Ane Books
Pvt. Ltd.

Springer

Group Theory

Dinesh Khattar · Neha Agrawal

Group Theory

Dinesh Khattar
Department of Mathematics
University of Delhi
New Delhi, India

Neha Agrawal
Department of Mathematics
University of Delhi
New Delhi, India

ISBN 978-3-031-21306-9 ISBN 978-3-031-21307-6 (eBook)
https://doi.org/10.1007/978-3-031-21307-6

Jointly published with Ane Books Pvt. Ltd.
In addition to this printed edition, there is a local printed edition of this work available via Ane Books in South Asia (India, Pakistan, Sri Lanka, Bangladesh, Nepal and Bhutan) and Africa (all countries in the African subcontinent).
ISBN of the Co-Publisher's edition: 978-93-90658-94-7

© The Author(s) 2023

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publishers, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publishers nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publishers remain neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Dedicated to our families as without their support it would not have been possible to write this book.

Preface

This book has been written as a text for undergraduate students of Mathematics. It is primarily based on the classroom lectures, the authors gave at the University of Delhi for many years. It is a near-impossible task, however, to cover, over the course of classroom lectures, the sheer volume of material that a student of group theory is called upon to master. The speed and capacity of understanding also varies from one student to another: while a committed student may grasp concepts without much assistance, another may require the teacher to invest more time and thought, and provide a greater number of illustrations. This book, therefore, is motivated by the need to supplement the classroom experience. It shall attempt to canvass a greater breadth of material than the class lectures, and it shall endeavor to cater to a broad spectrum of students in this process.

The book covers second and third-year group theory, in an undergraduate mathematics course, meeting the curriculum requirements of most Universities.

We have tried to present the subject matter in the language and tone of a classroom lecture. Thus the presentation is somewhat informal; we hope that this will put the readers at their ease.

Different concepts have been explained with the help of examples. The attempt is made by the authors to explain everything lucidly, so that it is possible to follow all the theories without the aid of a teacher.

Each Chapter opens with a short meditation on the rationale that propels our treatment of the subject being examined in that chapter. This is meant to furnish the student with insight into the overarching structure of the book, and to encourage an understanding of group theory as a cohesive body.

The book could be used for self study as well as for a course text, and so full details of almost all proofs are included along with hundreds of solved problems, to give ample guidance in understanding abstract notions. The solved problems are interspersed throughout the text at places where they naturally arise, making the book ideal for self-study. The proofs are precise and complete, backed up by chapter end problems, with just the right level of difficulty. There is plenty of scope for the readers to try and solve problems on their own. Also, the explanatory answers to the selected problems being given at the end of every chapter.

Important results in every chapter receive proportionate attention and emphasis; intermediate lemmas are also carefully designed so that they not only serve the theorems but are also valuable independently.

Each chapter contains 'Learning Objectives' which the reader would like to achieve after having gone through that chapter. This will help the students focus their study.

There are eleven chapters in this book starting with definition and examples of Groups. It then goes on to cover properties of groups, subgroups, Cyclic groups, Permutation groups, Cosets and Lagrange's Theorem, Normal subgroups and Factor Groups, Group Homomorphisms and Isomorphisms, Automorphisms, Direct Products, Group Actions and Sylow Theorems. A common thread runs through the entire book, tying each chapter to the next - the unifying thread being the treatment of the concept of symmetry of objects that do indeed satisfy the definition of a group.

We, gratefully, acknowledge the inspiration, encouragement and valuable suggestions received from the teachers who are teaching Group Theory in the undergraduate courses of several Universities. We also thank all our students for their curiosity for sharing with us the difficulties they experienced in learning these topics.

This work would not have been possible without the support and encouragement from Mr. Sunil Saxena and Mr. Jai Raj Kapoor at Ane Books.

Our sincere thanks and words of appreciation to all of them, who are directly or indirectly involved in the project.

We are grateful to our dear friend and colleague Dr. S. P. Tripathi who was generous, both with his time and his formidable intellect, and, in the course of a few short, incisive remarks, changed the path of this book entirely.

Last but not the least our young colleague Nishita, Assistant Professor, St. Stephens College, University of Delhi. We had the numbers, but she had the words, and her contributions are sprinkled throughout the pages of this work.

Suggestions and comments to improve the book in content and style are always welcome and will be greatly appreciated and acknowledged.

Thank you for choosing our book.

May you find it stimulating and rewarding.

Dinesh Khattar (Email: dkhattar@kmc.du.ac.in)
Neha Agrawal (Email: kmcneha@kmc.du.ac.in)

Foreword

Reading this marvelous book on Group Theory by Professor Dinesh Khattar and Dr. Neha Agrawal has brought back many pleasant memories. My first introduction to abstract mathematics occurred through Group Theory as a freshman undergraduate at Delhi University. I fell in love with the subject at once andl retain the same affection for Group Theory till today. I am also aware that one of the main reasons that caused me to fall in love with Group Theory was the fact that I had access to two outstanding books viz. Brikhoff and Maclane's classic 'A Survey of Modern Algebra' and I. N. Herstein's 'Topics in Algebra'. Thus, the role played by a good book in mastering a subject is vital. At the same time,I have had a nagging concern. There just haven't been too many scholarly yet interesting books on Group Theory authored by Indian mathematicians. One of the reasons for this concern is the fact that the plethora of good books that come into India from abroad are rather expensive and the not so expensive books by Indian authors generally tend not to be in the same league as the ones that come from abroad.

I am thus delighted to observe that Khattar and Agrawal's book on Group Theory fulfills the needs of India in many ways. More importantly, the book can prove to be quite useful to students across the globe. One of the most interesting features of the book is the fact that it blends history and mathematics in a meaningful way to arouse the interest of the student. The other very noteworthy feature of the book is that it is replete with examples and exercises of varying degrees of difficulty. This book illustrates concepts with a very large number of good examples and with just as many of exercises from the very easy to those that are challenging. The book is written in a very lucid and easy style that retains the interest of the reader throughout. The proofs are also very well explained. I am certain the book shall make a mark as a much needed text on Group Theory for undergradautes of mathematics, physics and chemistry.

There are three concepts that permeate all of mathematics in varying degrees: linearity, continuity and symmetry. This book is all about symmetry and written in a style that is as pleasing to the mind as symmetry is to the eyes. I commend the book wholeheartedly.

Prof. Dinesh Singh (Padma Shri)
Chancellor, K.R. Mangalam University
Formerly Vice Chancellor, University of Delhi
Distinguished Fellow of Hackspace, Imperial College London,
Adjunct Professor of Mathematics, University of Houston

Contents

Preface ..... *vii*
Foreword ..... *ix*
List of Symbols ..... *xiii*

1. Group 1–58
1.1 Groups 4
1.2 Cayley Table 8
1.3 Elementary Properties of Groups 32
1.4 Dihedral Groups 49

2. Finite Groups and Subgroups 59–98
2.1 Finite Groups 59
2.2 Subgroups 70
2.3 Subgroup Tests 71
2.4 Special Class of Subgroups 82
2.5 Intersection and Union of Subgroups 91
2.6 Product of Two Subgroups 93

3. Cyclic Groups 99–118
3.1 Cyclic Groups and their Properties 99
3.2 Generators of a Cyclic Group 102
3.3 Subgroups of Cyclic Groups 104

4. Permutation Groups 119–142
4.1 Permutation of a Set 119
4.2 Permutation Group of a Set 121
4.3 Cycle Notation 124
4.4 Theorems on Permutations and Cycles 126
4.5 Even and Odd Permutations 134
4.6 Alternating Group of Degree n 138

5. Cosets and Lagrange's Theorem 143–168
5.1 Definition of Cosets and Properties of Cosets 143
5.2 Lagrange's Theorem and its Applications 148
5.3 Application of Cosets to Permutation Groups 164

6. Normal Subgroups and Factor Groups 169–194
6.1 Normal Subgroup and Equivalent Conditions for a Subgroup to be Normal 169
6.2 Factor Groups 180
6.3 Commutator Subgroup of a Group and its Properties 187
6.4 The G/Z Theorem 189
6.5 Cauchy's Theorem for Abelian Group 191

7. Group Homomorphism and Isomorphism 195–222
7.1 Homomorphism of Groups and its Properties 195
7.2 Properties of Subgroups under Homomorphism 200
7.3 Isomorphism of Groups 205
7.4 Some Theorems Based on Isomorphism of Groups 207

8. Automorphisms 223–240
8.1 Automorphism of a Group 223
8.2 Inner Automorphisms 226
8.3 Theorems Based on Automorphism of a Group 228

9. Direct Products 241–270
9.1 External Direct Product 241
9.2 Properties of External Direct Products 244
9.3 $U(n)$ as External Direct Products 249
9.4 Internal Direct Products 254
9.5 Fundamental Theorem of Finite Abelian Groups 258

10. Group Actions 271–302
10.1 Group Actions 271
10.2 Kernels, Orbits and Stabilizers 275
10.3 Group acting on themselves by Conjugation 291
10.4 Conjugacy in Sn 296

11. Sylow Theorems 303–325
11.1 p–Groups and Sylow p–subgroups 303
11.2 Simple Groups 309

Index 327–329

List of Symbols

$\mathbb{N}$	:	set of natural numbers
$\mathbb{Z}$	:	set of integers
$\mathbb{Z}^+$	:	set of positive integers
$\mathbb{Q}$	:	set of rational numbers
$\mathbb{Q}^+$	:	set of positive rational numbers
$\mathbb{Q}^*$	:	set of non- zero rational numbers
$\mathbb{R}$	:	set of real numbers
$\mathbb{R}^+$	:	set of positive real numbers
$\mathbb{R}^*$	:	set of non- zero real numbers
$\mathbb{C}$	:	set of complex numbers
$\forall$	:	for all
$\exists$	:	there exist
$\in$	:	belong to
$\notin$	:	does not belong to
$\ni$	:	such that
$\subseteq$	:	subset of
$\subsetneq$	:	proper subset of
$\otimes_n$	:	multiplication modulo n
$\oplus_n$	:	addition modulo n
$\cong$	:	isomorphic to
$\ncong$	:	not isomorphic to
$\approx$	:	equivalence
$\leq$	:	subgroup
$\trianglelefteq$	:	normal subgroup
$\cap$	:	intersection
$\cup$	:	union
!	:	factorial
=	:	equal to
$\neq$	:	not equal to
$\Rightarrow$	:	implies
$\Leftrightarrow$	:	if and only if
$a\|b$	:	a divides b
$a\nmid b$	:	a does not divide b
lcm(a, b)	:	least common multiple of a and b
gcd(a, b)	:	greatest common divisor of a and b
det(A)	:	determinant of matrix A
$\wp(A)$	:	power set of A

1

Groups

Learning Objectives

- Concept of Symmetry
- Definition and Examples of Groups
- Cayley Table
- Elementary Properties of Groups
- Dihedral Groups

Concept of Symmetry

"Symmetry is a vast subject, significant in art and nature. Mathematics lies at its root, and it would be hard to find a better one on which to demonstrate the working of the mathematical intellect."

Thus unfolds a famous quote by the German mathematician Hermann Weyl. Weyl, above, refers to the fertile intersection of symmetry with mathematics, and that is where our project takes root as well. Nature and the cosmos supply us with limitless evidence of an inherent symmetry. When we look around ourselves, we discover that almost everything around us on earth is symmetrically fashioned. Both our arts and our sciences arise from a wide-eyed wonder at this miraculous inheritance. Our art seeks to synthesize this natural symmetry, while our science seeks to analyze it. Anything to do with symmetry in the sciences (physics, chemistry, biology) relies upon the mathematical tool called Group Theory†. Chemists, for instance, use symmetric groups to classify molecules and predict many of their chemical properties. Group theory, in fact, sends its branches into fields as fresh and exciting as modern cryptography, which widely employs symmetric groups as well.

† In 1958, Nobel Prize in Physics was awarded to 2 young Chinese Physicists Yang and Lee for discovering the anti-symmetry of particles using Group Theory.

© The Author(s) 2023

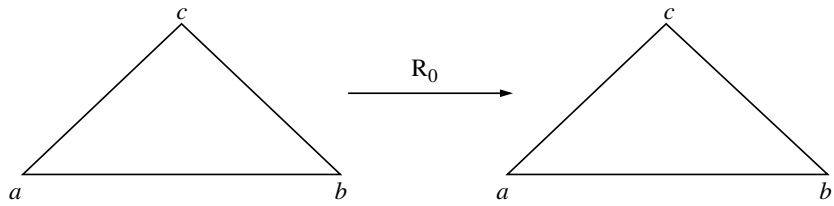
D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_1

What exactly is symmetry, then? Quite simply, it is this: when we say a certain shape is symmetric, or has symmetry, it means that we can fold the shape in half in such a way that both halves align exactly as they sit on top of each other. We mean that one half of the shape is a perfect match to the other. Mathematically, symmetry means that one shape becomes exactly like another when you move it in some way: turn, flip or slide.

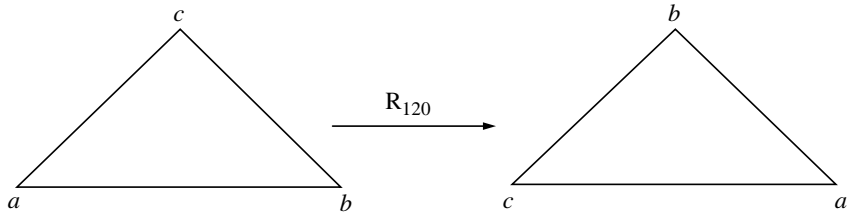
To begin with, consider an equilateral triangle. Suppose we remove it from the plane and move it in some way and then put it back into its original position. We need to see in how many possible ways this can be done.

To understand this let us mark the corners of the equilateral triangle as a, b and c. Consider all possible motions and try to relate the starting and the final positions.

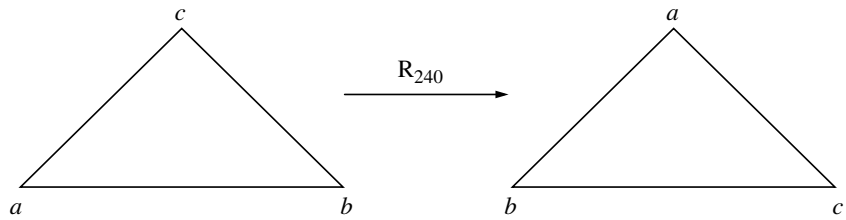
(i) Rotation of 0°:



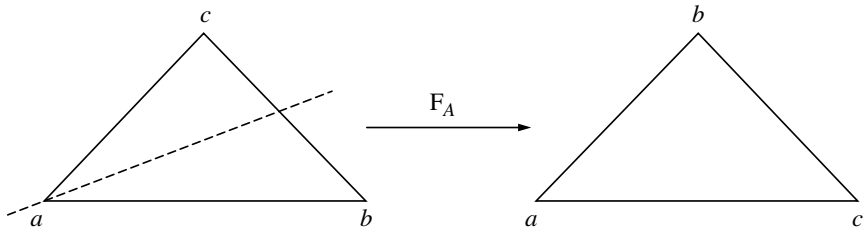
(ii) Rotation of 120°:



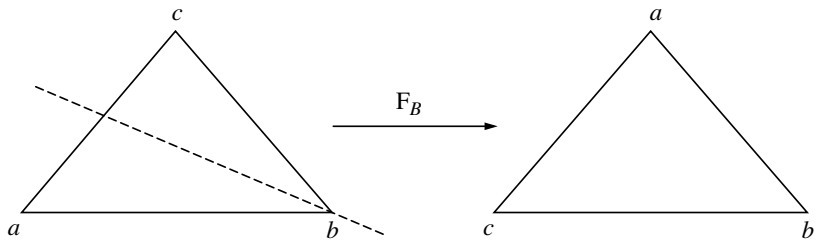
(iii) Rotation of 240°:



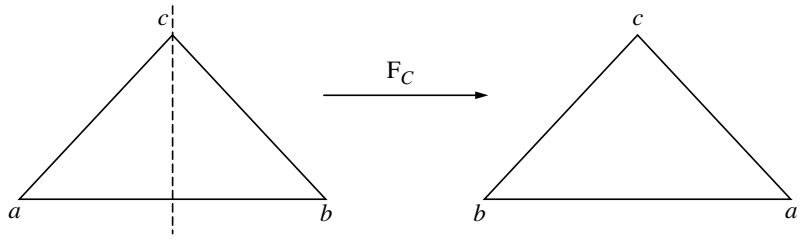
(iv) Reflection about the axis passing through the vertex a.



(v) Reflection about the axis passing through the vertex b.



(vi) Reflection about the axis passing through the vertex c.



We see that these are the only possible ways in which we can rotate or flip the triangle while retaining its original shape. Suppose we compose two possible motions say F_B followed by R_{240}. We observe that this gives a single motion F_C.

This tells us that composing any two motions gives back a single motion. These six motions can be viewed as functions from the set $A = \{a, b, c\}$ to itself.

Let us write these elements in set form as

$$S = \{R_0, R_{120}, R_{240}, F_A, F_B, F_C\}$$

Out of these six elements, three elements are rotations and three are reflections.

These elements of S being functions can be composed by function composition to yield another function.

$$fg(x) = f(g(x)) \quad \text{for all} \quad x \in A.$$

For example: $F_AF_B(a) = c$, $F_AF_B(b) = a$, $F_AF_B(c) = b$. Thus $F_AF_B = R_{120}$.

For convenience, let us make a multiplication table as

	R_0	R_{120}	R_{240}	F_A	F_B	F_C
R_0	R_0	R_{120}	R_{240}	F_A	F_B	F_C
R_{120}	R_{120}	R_{240}	R_0	F_C	F_A	F_B
R_{240}	R_{240}	R_0	R_{120}	F_B	F_C	F_A
F_A	F_A	F_B	F_C	R_0	R_{120}	R_{240}
F_B	F_B	F_C	F_A	R_{240}	R_0	R_{120}
F_C	F_C	F_A	F_B	R_{120}	R_{240}	R_0

This table is also called **Cayley Table**, which will be discussed in detail later in this chapter.

Studying the table, we observe some interesting things like composing any two entries of the set we again get an element from the same set without introducing any new element. This property is known as **closure** and S is said to be closed here. Also, we observe that composing any function with R_0 either from left or right yields the same function. This element R_0 is called the **identity element** because it never changes the behavior of any function it is composed with.

Further looking at every column of the table we see that corresponding to every element h in S, there is some element k again from S that neutralizes the effect of h and gives the identity R_0. Such an element k is called the **inverse** of h.

Also, we know function composition is **associative** in nature. Therefore, the set S has four properties, namely closure, associativity, identity and inverse.

Any algebraic structure which satisfies the above four axioms, namely closure, associativity, identity and inverse, is called a **group**, which will be formally defined later.

The set S defined above together with the operation of function composition satisfies all the group properties and hence is a group called a **Dihedral group**.

The Dihedral groups are a very important class of groups that will be discussed in detail towards the end of this chapter.

1.1 Groups

In this section we formally define an algebraic structure named as **Group**. Algebraic structures are those non-empty sets, together with binary composition, that satisfy one or more axioms. One of the simplest and most basic of all algebraic structures is the group. Numerous examples of groups are discussed. These examples will be used throughout this book. We therefore study these examples in details.

Before we begin with the formal definition of a group, we recall the definition of a binary composition.

Definition 1.1: A **binary composition** '$*$' on a non-empty set G is a function from $G \times G$ into G, i.e., $* : G \times G \to G$ such that $\forall\ a, b \in G$, we have $a * b \in G$.

Note that if $*$ is a binary composition on a set G, then we say that G is closed under the operation $*$.

Intuitively, a binary operation on a set G is a way of combining any two elements of G to produce another element in the same set G.

We now give some examples.

Example 1.1: Consider the set $\mathbb{Z}$ of integers.

The operation $*$ defined by $a * b = a + b$ for all $a, b \in \mathbb{Z}$ is a binary composition. Similarly, the compositions defined by $a * b = a - b$ and $a * b = a \cdot b$ for all $a, b \in \mathbb{Z}$ are binary compositions.

However $a * b = \frac{a}{b}$ may not belong to $\mathbb{Z}$ for every $a, b \in \mathbb{Z}$, so division of integers in not a binary composition.

Definition 1.2: A non-empty set G together with one or more binary operations is called an **algebraic structure.**

The algebraic structure consisting of a non-empty set G together with a binary composition $*$ is denoted by $(G, *)$.

Example 1.2: Define $*$ on $\mathbb{Z}$ by $a * b = a + b$, $\forall\ a, b \in \mathbb{Z}$. Then, $*$ is a binary composition in the set E of all even integers but $*$ is not a binary composition in the set O of odd integers, since $11, 13 \in O$ but $11 + 13 = 24 \notin O$.

Let us now define a group.

Definition 1.3: A non-empty set G, together with a binary composition $*$, is said to form a **group** if it satisfies the following axioms, called the group axioms:

(i) **Associativity:**

$$a * (b * c) = (a * b) * c, \quad \forall a, b, c \in G$$

It means the two possible ways of combining three elements (without changing their order) yield the same result.

(ii) **Existence of Identity:** For every element $a \in G$, there exists an element $e \in G$ such that

$$a * e = e * a = a.$$

The element e is called **identity** or **neutral** element of G, for it may be combined with any element a without altering a.

(iii) **Existence of Inverse:** For every $a \in G$, there exists $a' \in G$ such that

$$a * a' = a' * a = e\ .$$

It means the combination of any element with its **inverse** produces the neutral element, i.e., the inverse of a "neutralizes" a.

The element a' is called inverse of a and it is denoted by a^{-1}.

So, by a group we mean any set, with any associative binary operation, having a neutral element and allowing each element an inverse.

The group we have just defined is an algebraic structure and therefore is represented by the symbol $(G, *)$. This notation makes it explicit that the group consists of the set G and the operation $*$.

For the sake of simplicity, we write ab instead of $a * b$.

We now define an **Abelian Group** (named after great Norwegian Mathematician Niels Abel, who was a pioneer in the study of groups) or a **Commutative Group**.

Definition 1.4: A group $(G, *)$ is said to be an **abelian group** or **a commutative group** if

$$a * b = b * a \qquad \forall a, b \in G.$$

A group G is non-abelian, if there exist pair of elements a and b in G for which

$$a * b \neq b * a.$$

Definition 1.5: A group G is said to be **finite** if the set G is finite, else it is **infinite**.

Definition 1.6: An algebraic structure $(G, *)$ is called a **groupoid** or **quasi-group**, if $a * b \in G$, $\forall\ a, b \in G$, i.e., G is closed for the binary operation.

Definition 1.7: An algebraic structure $(G, *)$ is called a **semi-group** if the binary operation $*$ is associative in G, i.e.,

$$(a * b) * c = a * (b * c)\ \forall\ a, b, c \in G$$

Definition 1.8: An algebraic structure $(G, *)$ is called a **monoid** if

(i) the binary operation $*$ is associative in G, i.e.,

$$(a * b) * c = a * (b * c)\ \forall\ a, b, c \in G, \text{ and}$$

(ii) there exists an identity element in G.

Clearly, a group $(G, *)$ is a monoid in which every element has an inverse.

We now consider a few examples of systems that form groups and also systems that do not form groups.

Example 1.3: Let $G = \mathbb{Z}$, the set of integers.

Define the operation $*$ on G by $a * b = a + b$ for all $a, b \in G$.

(i) **Closure:** $\forall a, b \in G$, we have, $a * b = a + b \in G$. So, closure holds.

(ii) **Associativity:** Since addition of integers is associative, i.e., $\forall\ a, b, c \in G$, we have $(a + b) + c = a + (b + c)$,
Therefore, associativity holds.

(iii) **Identity:** The element $0 \in G$ is the identity element as

$$\forall\ a \in G, \quad a + 0 = a = 0 + a$$

(iv) **Inverse:** For every element a in the group G, there exists some element $(-a) \in G$ such that

$$a + (-a) = 0 = (-a) + a$$

The element $a^{-1} = (-a) \in G$ is the inverse of a.

Thus, $(G, +)$ forms a group.

Also, since integers are commutative under addition for all a, b in G, we have

$$a + b = b + a$$

Hence $(G, +)$ is an abelian group.

In fact $(G, +)$ is an infinite abelian group, as the set G is infinite.

Remarks:

- The set of rational numbers $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$ form abelian groups under ordinary addition.
  In each case the identity element is 0 and the inverse of a is $-a$.
- The set of integers under subtraction does not form a group as associativity does not hold. For example, $2 - (-3 - 4) \neq (2 - (-3)) - 4$.

Example 1.4: Let $G = \mathbb{Z}$, the set of integers. Define the composition $*$ on G by

$$a * b = a \cdot b \quad \text{for all} \quad a, b \in G$$

(i) **Closure:** Since for every $a, b \in G$, we have, $a * b = a \cdot b \in G$, therefore G is closed under multiplication.

(ii) **Associativity:** Since multiplication of integers is associative, i.e.,

$$\forall a, b, c \in G, \quad (a \cdot b) \cdot c = a \cdot (b \cdot \mathrm{c}),$$

$\therefore$ Associativity holds.

(iii) **Identity:** The element $1 \in G$ is the identity element of G as

$$\forall\, a \in G, \quad a \cdot 1 = a = 1 \cdot a$$

(iv) **Inverse:** For every element $a \in G$, we have $a \cdot 1/a = 1 = 1/a \cdot a$, but it may happen that $1/a$ does not belong to G.
In the case when $G = \mathbb{Z}$, the element $1/a$ is not in G for every $a \neq -1, 1$. Hence, a^{-1} may not exist for every element a in G.

Thus, $(G, *)$ is not a group.

Remarks:

- The set of real numbers or rational numbers is not a group under multiplication, as the element 0 does not have a multiplicative inverse.
- Any set containing 0 is not a group under multiplication.

Example 1.5: The set $\mathbb{Q}^+$ of positive rational numbers is a group under ordinary multiplication. The inverse of any element a is $1/a = a^{-1}$.

In fact, $(\mathbb{Q}^+, \cdot)$ is an abelian group.

Example 1.6: The set $\mathbb{R}^*$ of non-zero real numbers is an abelian group under ordinary multiplication. The identity is 1. The inverse of a is $1/a$ for all a in $\mathbb{R}^*$.

Example 1.7: The set $\mathbb{N}$ of all natural numbers is not a group under the composition of ordinary addition as there exists no b in $\mathbb{N}$ such that $a + b = a = b + a$, for every $a \in \mathbb{N}$.

Example 1.8: The set S of positive irrational numbers together with 1, under multiplication, satisfies the three properties given in the definition of a group, but is not a group. Indeed, $\sqrt{2} \cdot \sqrt{2} = 2 \notin S$, so S is not closed under multiplication.

Example 1.9: The set $\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n): a_i \in \mathbb{R}\}$ forms an abelian group under the operation of component-wise addition.

Here, (0, 0, ..., 0) is the identity element and $(-a_1, -a_2, \ldots, -a_n) \in \mathbb{R}^n$ is the inverse of $(a_1, a_2, \ldots, a_n)$.

Problem 1.1 Prove that the set of all rational numbers of the form $3^m \cdot 6^n$, where m and n are integers, is a group under multiplication.

Solution Let $G = \{3^m \cdot 6^n \in \mathbb{Q} : m, n \in \mathbb{Z}\}$

Let $3^m \cdot 6^n \in G$ and $3^{m_1} \cdot 6^{n_1} \in G$, then

$$(3^m \cdot 6^n)(3^{m_1} \cdot 6^{n_1}) = 3^{m+m_1} \cdot 6^{n+n_1} \in G \quad \text{as} \quad m + m_1, n + n_1 \in \mathbb{Z}$$

$\therefore$ Closure property holds.

Since the set of rational numbers is associative under multiplication, therefore associativity holds in G.

Also, $1 = 3^0 \cdot 6^0 \in G$ such that

$$(3^0 \cdot 6^0)\ (3^m \cdot 6^n) = 3^m \cdot 6^n = (3^m \cdot 6^n)\ (3^0 \cdot 6^0)$$

$\therefore$ $1 \in G$ is the identity element.

Inverse of $3^m \cdot 6^n \in G$ is $3^{-m} \cdot 6^{-n} \in G$ as $-m, -n \in \mathbb{Z}$ such that

$$(3^m \cdot 6^n)\ (3^{-m} \cdot 6^{-n}) = 1 = (3^{-m} \cdot 6^{-n})\ (3^m \cdot 6^n)$$

Thus, G is a group under multiplication.

1.2 Cayley Table

In the above examples, we have taken the set G to be an infinite set. In case of finite sets of small order, to prove that G is closed under the given operation, it is convenient to make a composition table called **Cayley table**†.

Let G be a non-empty finite set, say, $G = \{a_1, a_2, \ldots, a_n\}$ with a binary composition $*$. In order to prepare the composition table, we write all the elements of G horizontally in a row and vertically in a column as shown below. Then $a_i * a_j$ is the element that occurs at the intersection of ith row and j^{th} column.

† It is named after the 19th century British mathematician Arthur Cayley. A Cayley table describes the structure of a finite group by arranging all the possible products of all the group elements in a square table. Many properties of the group—such as whether or not it is abelian, which elements are inverses of which elements, what is the identity element and so on, can be discovered from its Cayley table.

$*$	a_1	a_2	a_3	—	—	a_j
a_1	$a_1 * a_2$	$a_1 * a_2$	$a_1 * a_3$	—	—	$a_1 * a_j$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$	—	—	$a_2 * a_j$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$	—	—	$a_3 * a_j$
—	—	—	—	—	—	—
—	—	—	—	—	—	—
a_i	$a_i * a_1$	$a_i * a_2$	$a_i * a_3$	—	—	$a_i * a_j$

Note that if all the elements $a_i * a_j$ are in G, then $*$ is a binary operation.

Also, every group table is a **Latin square**, that is, each element of the group appears exactly once in each row and each column.

We explain this table in the next few examples.

Example 1.10: The subset $G = \{1, -1, i, -i\}$of the set of complex numbers is a group under usual complex multiplication. In fact, it is a finite abelian group.

(i) **Closure:** The closure is established through the following composition table

Table 1.1: The Cayley Table of G

.	1	–1	i	$-i$
1	1	–1	i	$-i$
–1	–1	1	$-i$	i
i	i	$-i$	–1	1
$-i$	$-i$	i	1	–1

Clearly, from the Cayley table given above, it can be seen that the closure property holds, since for every a, b in G, the element $a \cdot b$ is also in G.

(ii) **Associativity:** Since complex numbers are associative with respect to multiplication, therefore associativity holds.

(iii) **Identity:** $1 \in G$ is the identity element as $\forall\ a \in G$, $a \cdot 1 = a = 1 \cdot a$.

(iv) **Inverse:** Since 1.1 = 1, –1. –1 = 1, i. $-i$ = 1 and $-i$. i = 1, the inverse of 1, –1, i, $-i$ are 1, –1, $-i$, i respectively.

Therefore, G forms a finite group under complex multiplication.

Also, since for every $a, b \in G$, we have $a \cdot b = b \cdot a$, therefore $(G, .)$ is an abelian group.

Remark: The numbers 1, –1, i, $-i$, where $i^2 = -1$ are the four fourth roots of unity. Thus, the four fourth roots of unity form a finite abelian group of order 4 with respect to multiplication.

Example 1.11: We now consider an important non-abelian group called the group of Quaternions†. It is a finite group consisting of 8 elements $1, -1, i, -i, j, -j, k, -k$.

Let $G = Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

Define composition on G by using multiplication as

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

(i) **Closure:** The closure is established through the following composition table

Table 1.2: The Cayley Table of G

·	1	–1	i	$-i$	j	$-j$	k	$-k$
1	1	–1	i	$-i$	j	$-j$	k	$-k$
–1	–1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	–1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	–1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	–1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	–1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	–1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	–1

Clearly from the Cayley table given above, closure property holds.

(ii) **Associativity:** Clearly, $\forall a, b, c \in G$, we have $(ab)c = a(bc)$, therefore, associativity holds.

(iii) **Identity:** $1 \in G$ is the identity element as $a \cdot 1 = a = 1 \cdot a\ \forall\ a \in G$

(iv) **Inverse:** Since, $1.1 = 1, -1.\ -1 = 1, i.\ -i = 1, -i.\ i = 1$

$$j.\ -j = 1, -j.\ j = 1, k.\ -k = 1, -k.\ k = 1,$$

therefore inverse of 1 is 1, –1 is –1, i is $-i$, $-i$ is i, j is $-j$, $-j$ is j, k is $-k$ and $-k$ is k.

Hence, $(G, .)$ is a group.

It is not an abelian group as $ij = -ji$, so $ij \neq ji$.

As already mentioned, this group is called the **Quaternion Group.**

Thus, Q_8 is an example of a finite non- abelian group.

† In mathematics, the quaternions are a number system that extends the complex numbers. They were first described by Irish mathematician William Hamilton in 1843. They have practical uses in applied mathematics—in particular for calculations involving three-dimensional rotations such as in computer graphics and texture analysis.

PROBLEM 1.2 Prove that the set $G = \{1, \omega, \omega^2\}$, where ω is an imaginary cube root of unity, is a finite abelian group under multiplication.

SOLUTION Note that $\omega^3 = 1$.

The composition table is given below:

Table 1.3: Group Table of G

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

1. Since all the entries in the composition table are elements of the set G, therefore G is closed w.r.t. multiplication.
2. Since the elements of G are all complex numbers and multiplication of complex numbers is associative, therefore associativity holds.
3. Clearly from the Cayley table, we have
$$1 \cdot 1 = 1, \quad 1 \cdot \omega = \omega = \omega \cdot 1, \quad 1 \cdot \omega^2 = \omega^2 = \omega^2 \cdot 1$$
Therefore, $1 \in G$ is the identity element.
4. Also, from the table, the inverses of 1, ω, ω^2 are 1, ω^2, ω respectively.

Therefore, G forms a finite group under multiplication.

Since multiplication of complex numbers is commutative, therefore G is a finite abelian group under multiplication.

PROBLEM 1.3 If the table given below is a group table, fill in the blank entries.

Table 1.4: Group Table

	e	a	b	c	d
e	e	–	–	–	–
a	–	b	–	–	e
b	–	c	d	e	–
c	–	d	–	a	b
d	–	–	–	–	–

SOLUTION We have from group table

$aa = b, ba = c, bb = d, bc = e, ee = e, ad = e, ca = d, cc = a, cd = b$.

Since $ad = e$, we get that

$$da = e$$

Also as $bc = e$, this gives

$$cb = e.$$

Again, since $ee = e$, we have

$$ae = a,\ be = b,\ ce = c,\ de = d.$$

This implies that $ea = a,\ eb = b,\ ec = c,\ ed = d.$

Also $ba = c$ gives $ab = c$ and $ca = d$ implies $ac = d$.

Since $a^2 = b,\ b^2 = d$ and $c^2 = a$, we get that $bb = ba^2$.

Since $bd = db = bb^2 = bba^2 = b^2\ a^2 = b^2\ c^4 = c^4\ b^2 = c^2ccbb$

$= c^2\,ceb = c^2\ cb,$ we have $bd = db = c^2 = a.$

Thus, we have

Table 1.5: Final Group Table

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

PROBLEM 1.4 Show that the set $G = \{x + y\sqrt{5} : x, y \in \mathbb{Q}\}$ forms a group under addition.

SOLUTION Let $a = x_1 + y_1\sqrt{5}$, $b = x_2 + y_2\sqrt{5}$ and $c = x_3 + y_3\sqrt{5}$ be any three elements of G, where $x_i, y_i \in \mathbb{Q}$ for $i = 1, 2, 3$.

(i) Closure: We have

$$a + b = (x_1 + y_1\sqrt{5}) + (x_2 + y_2\sqrt{5}) = (x_1 + x_2) + (y_1 + y_2)\sqrt{5} \in G$$

as $x_1 + x_2 \in \mathbb{Q}$ and $y_1 + y_2 \in \mathbb{Q}$

(ii) Associativity: We have

$$(a + b) + c = ((x_1 + y_1\sqrt{5}) + (x_2 + y_2\sqrt{5})) + (x_3 + y_3\sqrt{5})$$

$$= ((x_1 + x_2) + (y_1 + y_2)\sqrt{5}) + (x_3 + y_3\sqrt{5})$$

$$= ((x_1 + x_2) + x_3) + ((y_1 + y_2) + y_3)\sqrt{5}$$

$$= (x_1 + (x_2 + x_3)) + (y_1 + (y_2 + y_3))\sqrt{5}$$

by associativity in $\mathbb{Q}$

$$= (x_1 + y_1\sqrt{5}) + ((x_2 + x_3) + (y_2 + y_3)\sqrt{5})$$

$$= (x_1 + y_1\sqrt{5}) + ((x_2 + y_2\sqrt{5}) + (x_3 + y_3\sqrt{5}))$$

$$= a + (b + c)$$

Therefore, associativity holds.

(iii) Identity: $0 + 0\sqrt{5} \in G$ is the identity as

$$(x + y\sqrt{5}) + (0 + 0\sqrt{5}) = (x + y\sqrt{5}) = (0 + 0\sqrt{5}) + (x + y\sqrt{5})$$

$$\forall x + y\sqrt{5} \in G$$

(iv) Inverse: For all $x + y\sqrt{5} \in G$ there exist $-x - y\sqrt{5} \in G$ such that

$$(x + y\sqrt{5}) + (-x - y\sqrt{5}) = (0 + 0\sqrt{5}) = (-x - y\sqrt{5}) + (x + y\sqrt{5})$$

Therefore, $-x - y\sqrt{5} \in G$ is the inverse of $x + y\sqrt{5} \in G$

Thus, G forms a group under addition.

Example 1.12: Let $G = \{A : A \text{ is } 2 \times 2 \text{ matrix over } \mathbb{R}\}$.

Then, G forms a group under matrix addition.

(i) Let $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in G$

Then, $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \in G.$

(ii) Matrix addition is always associative.

(iii) The identity element is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in G$

(iv) The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in G$.

Thus G forms a group under matrix addition. Since matrix addition is commutative, therefore G is an abelian group.

Example 1.13: Let $G = \{A : A \text{ is } 2 \times 2 \text{ matrix over } \mathbb{R} \text{ with } |A| \neq 0\}$.

Then G is a group under matrix multiplication.

(i) Let $A, B \in G$, then $|A| \neq 0$ and $|B| \neq 0$.

$\therefore \quad |AB| = |A|\,|B| \neq 0$

$\therefore \quad AB \in G.$

(ii) Matrix multiplication is always associative.

(iii) Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then since $|I| = 1 \neq 0$, we have $I \in G$.

Also $\quad AI = A = IA, \ \forall A \in G.$

Therefore I is the identity element of G.

(iv) We also have for $A \in G$, $A \cdot adj\ A = |A| I = adj\ A \cdot A$

$$\Rightarrow \quad A\left(\frac{1}{|A|} adj\ A\right) = I = \left(\frac{1}{|A|} adj\ A\right) A$$

Thus $\quad A^{-1} = \frac{1}{|A|} adj\ A \in G$

Therefore G is a group under matrix multiplication.

Remark: We write $G = GL(2, \mathbb{R})$ = General Linear Group of 2×2 matrices A with real entries such that $|A| \neq 0$.

In the next problem, we show that the group $GL(2, \mathbb{R})$ is non-abelian.

Problem 1.5 Show that the group

$$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

is non-abelian.

Solution

Let $\quad A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ be any two elements in the group $GL(2, \mathbb{R})$.

Then $\quad AB = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$ ...(1)

and $\quad BA = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} a_2a_1 + b_2c_1 & a_2b_1 + b_2d_1 \\ c_2a_1 + d_2c_1 & c_2b_1 + d_2d_1 \end{bmatrix}$ ...(2)

From (1) and (2), we get $AB \neq BA$.

Therefore, the group $GL(2, \mathbb{R})$ is non-abelian.

Example 1.14: The set of all 2×2 matrices with real entries is not a group under matrix multiplication, as inverse of a matrix A does not exist when $|A| = 0$.

Example 1.15: Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in \mathbb{R}, a \neq 0 \right\}$. Then, G forms an abelian group with respect to matrix multiplication.

(i) Let $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}, B = \begin{pmatrix} b & b \\ b & b \end{pmatrix} \in G.$

Then as $a \neq 0$ and $b \neq 0$, we have $ab \neq 0$.

$\therefore \quad AB = \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} \in G.$

Hence, G is closed.

(ii) Matrix Multiplication is always associative.

(iii) Let $\begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$ be the identity element

Then $\begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$ gives $\begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$

$\Rightarrow \quad 2ab = a \quad \text{or} \quad b = \frac{1}{2}$

$\therefore \quad \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix}.$

Thus, $\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \in G$ is the identity element.

(iv) Let $\begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$ be the inverse of $\begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G$

Then, $\begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \Rightarrow \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$

$\Rightarrow \quad 2ab = \frac{1}{2} \quad \text{or} \quad b = \frac{1}{4a}$

$\therefore \quad \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix}.$

$\therefore \quad \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix} \in G$ is the inverse of the matrix $\begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G.$

Thus, G forms a group under matrix multiplication.

Clearly, G is abelian because $AB = BA$ for all $A, B \in G$.

Remarks: We make two observations from the above example:

- Though matrix multiplication is not commutative, there is a subset of the set of matrices which forms an abelian group.
- If the determinant of a matrix is zero, then also it can be invertible (with respect to some identity element). Note that this is so because in this case, the identity element is not the usual unit matrix I_2.

To understand this, let us consider the following problem:

Problem 1.6 Let $G = \left\{ \begin{bmatrix} a & 0 \\ 2a & 0 \end{bmatrix} : a \in \mathbb{Q},\ a \neq 0 \right\}$ Show that G is a group with respect to matrix multiplication.

Solution Here, $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \in G$ is the identity for G, $\begin{bmatrix} 1/a & 0 \\ 2/a & 0 \end{bmatrix} \in G$ is the inverse of $\begin{bmatrix} a & 0 \\ 2a & 0 \end{bmatrix} \in G$.

In fact, G is an abelian group.

Remark: For simplicity, we have restricted our matrix examples to the 2×2 case. However, these can be easily generalized to $n \times n$ matrices.

Problem 1.7 Show that the set of all 3×3 matrices of the form

$$\left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$$

is a group with respect to matrix multiplication.

Solution

(i) Let $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} \in G$

Then, $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{bmatrix} \in G$

$\therefore$ Closure property is satisfied.

(ii) G is associative as matrix multiplication is associative.

(iii) Now, $$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in G.$$

Since $AI = A = IA$, therefore I is the identity element of G.

(iv) Let $$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\Rightarrow \quad \begin{bmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\Rightarrow \quad a + a' = 0,\ c + c' = 0 \quad \text{and} \quad b' + a(-c) + b = 0.$$

This gives $a' = -a$, $c' = -c$ and $b' = ac - b$

$$\therefore \quad \text{inverse of } \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in G \text{ is } \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \in G.$$

Hence, G forms a group.

This group is called **Heisenberg group**†.

Problem 1.8 Show that the set of matrices

$$G = \left\{ \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} : \alpha \in R \right\}$$

forms a group under matrix multiplication.

Solution

(i) Closure property:

Let $$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \text{ and } A_\beta = \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} \in G$$

Then, $$A_\alpha A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}\begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta} \in G$$

† Heisenberg group is important as it is used in the description of one-dimensional quantum mechanical systems

(ii) We know that matrix multiplication is associative.

(iii) $A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ is the identity element as

$$A_\alpha A_0 = A_\alpha = A_0 A_\alpha \quad \forall\ A_\alpha \in G$$

(iv) Clearly for all $A_\alpha \in G$ there exist $A_{-\alpha} \in G$ such that $A_\alpha A_{-\alpha} = A_0 = A_{-\alpha} A_\alpha$

$\therefore$ $A_{-\alpha} \in G$ is the inverse of $A_\alpha \in G$.

Hence G forms a group under matrix multiplication.

Problem 1.9 Show that the set G of all positive rational numbers is an abelian group under the binary operation $*$ defined by

$$a * b = \frac{ab}{2},\ a, b \in G\ .$$

Solution Closure follows as $a * b = \frac{ab}{2} \in G$, $\forall\ a, b \in G$.

$$(a * b) * c = \frac{ab}{2} * c = \frac{(ab)c}{4} = \frac{a(bc)}{4} = a * \frac{bc}{2} = a * (b * c) \quad \forall a,b,c \in G$$

Therefore, associativity holds,

$2 \in G$ is the identity and $4/a \in G$ is the inverse of any element $a \in G$.

Also, $$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a \quad \forall\ a, b \in G$$

Therefore, G is an abelian group under the given binary operation $*$.

Remarks: We now recall some useful results in number theory to be used in the next set of examples.

- **Division algorithm:** Let a and b be integers with $b > 0$. Then, there exists unique integers q and r such that $a = bq + r$, $0 \le r < b$.
- We say b divides a if and only if $r = 0$, i.e., b divides a if and only if $a = bq$
- The greatest common divisor (gcd) of two integers a and b is the largest of all common divisors of a and b, i.e., $\gcd(a, b) = d$ if and only if
  (a) d/a and d/b
  (b) If k/a and k/b, then $k \le d$.
- a and b are said to be relatively prime if and only if $\gcd(a, b) = 1$.
- If $\gcd(a, b) = 1$, then there exist integers x and y such that $ax + by = 1$.
- We have $a \equiv b \bmod n$, whenever n divides $b - a$.

Example 1.16: Let n be a positive integer. Let $\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-1\}$.

For $a, b \in \mathbb{Z}_n$, define the operation $\oplus_n$ in $\mathbb{Z}_n$ as $a \oplus_n b = c$, where c is the remainder obtained on dividing $a + b$ by n.

Illustration: For $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, Cayley table for $\mathbb{Z}_4$ is

Table 1.6: Cayley Table for $\mathbb{Z}_4$

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Since all the axioms of a group are satisfied, therefore, $(\mathbb{Z}_4, \oplus_4)$ is a group.

We now show that $(\mathbb{Z}_n, \oplus_n)$ is a group.

(i) **Closure:** For $a, b \in \mathbb{Z}_n$, we have

$$a + b = nq + c, 0 \leq c < n$$

Therefore, $c \in \mathbb{Z}_n$.

Since, $a \oplus_n b = c$, $\therefore\ a \oplus_n b \in \mathbb{Z}_n$, and hence closure holds.

(ii) **Associativity:** Let $a, b, c \in \mathbb{Z}_n$, then

$$\begin{aligned}(a \oplus_n b) \oplus_n c &= ((a + b) (\mathrm{mod}\, n) + c) (\mathrm{mod}\, n) \\ &= ((a + b) + c) (\mathrm{mod}\, n) \\ &= (a + (b + c)) \bmod n \text{ (since addition of integers is associative)} \\ &= (a + (b + c) (\mathrm{mod}\, n)) (\mathrm{mod}\, n) \\ &= a \oplus_n (b \oplus_n c)\end{aligned}$$

Thus, associativity holds.

(iii) **Identity:** Since $a \oplus_n 0 = a = 0 \oplus_n a,\ \forall a \in \mathbb{Z}_n$. Therefore, 0 is the identity element in $\mathbb{Z}_n$.

(iv) **Inverse:** Since $0 \oplus_n 0 = 0$, inverse of 0 is 0.

Let $0 \neq a \in \mathbb{Z}_n$. Then $0 < a < n$ so that $0 < n - a < n$.

Hence $(n - a) \in \mathbb{Z}_n$ such that $a \oplus_n (n - a) = 0 = (n - a) \oplus_n a$

Thus, $(n - a)$ is the inverse of a.

Therefore $(\mathbb{Z}_n, \oplus_n)$ is a group.

Also since $a \oplus_n b = b \oplus_n a, \quad \forall a, b \in \mathbb{Z}_n$, therefore $(\mathbb{Z}_n, \oplus_n)$ is an abelian group.

The operation $\oplus_n$† is usually referred to as addition modulo n. That is why, this group is usually referred to as the **group of integers under addition modulo n**.

Caution: If we exclude 0 from the above set, it will not form a group.

Example 1.17: Let $U(n) = \{x \in \mathbb{Z} : 1 \le x < n, \gcd(x, n) = 1\}$

We define a binary composition $\otimes_n$ on $U(n)$ by $a \otimes_n b = c$, where c is the least positive remainder obtained when $a \cdot b$ is divided by n.

The composition $\otimes_n$ is called **multiplication modulo n**.

Illustration: Consider $U(8) = \{1, 3, 5, 7\}$. Then, under multiplication modulo 8, the Cayley table is

Table 1.7: Cayley Table under multiplication modulo 8

$\otimes_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

It can be seen from the above table that for every $a, b \in U(8)$, $a \otimes_8 b \in U(8)$. The element $1 \in U(8)$ is the identity element. Also, the inverse of 1, 3, 5, 7 is 1, 3, 5 and 7 respectively.

Hence $(U(8), \otimes_8)$ is a group.

We will now show that $(U(n), \otimes_n)$ forms a group.

(i) **Closure:** For $a, b \in U(n)$, let $a \otimes_n b = c$.

To show that $c \in U(n)$, we need to prove that $1 \le c < n$ and $\gcd(c, n) = 1$.

We have, $ab = nq + c, \quad 0 \le c < n.$

If $c = 0$, then $ab = nq$

$\therefore$ n/ab implying n/b as $\gcd(a, n) = 1$

† Clearly, by definition of $\oplus_n$

$$a \oplus_n b = \begin{cases} a+b, & \text{if } a+b<n \\ a+b-n, & \text{if } a+b \ge n \end{cases}$$

This contradicts the fact that $\gcd(b, n) = 1$

$\therefore \quad c \neq 0$ and hence $1 \leq c < n$.

Also, c, n are co-prime, because if c, n are not co-prime, then there exists some prime p such that p/c and p/n.

Again as $ab = nq + c$ for some q,

we get p/ab ($\because$ p/n gives p/nq, $p/c \Rightarrow p/nq + c$)

Now, since p is prime, we have either p/a or p/b.

If p/a, then as p/n, it means a, n are not co-prime, a contradiction, as a, n are co-prime.

Similarly p/b leads to a contradiction.

Hence c, n are co-prime and thus $c \in U(n)$, showing that closure property holds.

(ii) **Associativity:** Let $a, b, c \in U(n)$. Then

$$a \otimes_n (b \otimes_n c) = (a(bc \pmod n)) \pmod n = a(bc) \pmod n$$
$$= (ab)c \pmod n, \quad \text{since multiplication in } \mathbb{Z} \text{ is associative}$$
$$= ((ab \pmod n)c) \pmod n = (a \otimes_n b) \otimes_n c$$

Thus, $\otimes_n$ is associative.

(iii) **Identity:** It is easy to see that $a \otimes_n 1 = 1 \otimes_n a = a, \quad \forall a \in U(n)$.

So, 1 acts as identity of $U(n)$.

(iv) **Inverse:** Let $a \in U(n)$ be any element, then a and n are co-prime and thus we can find integers x and y such that $ax + ny = 1$ ...(1)

By division algorithm, we can write $x = qn + r$, where $0 \leq r < n$

If $r = 0$, then $x = qn$, so by (1), we get, $aqn + ny = 1$,

i.e., $n(aq + y) = 1$. This is not possible as $n > 1$ and $aq + y$ is an integer.

Hence, $r \neq 0$, i.e., $1 \leq r < n$.

Also, r, n are co-prime, because if r, n are not co-prime, we can find a prime number p such that p/r, p/n

$\Rightarrow$ p/qn and p/r, therefore $p/qn + r$ implying p/x

$\Rightarrow$ p/ax. Also, p/ny

$\Rightarrow$ $p/ax + ny = 1$, which is not possible.

Thus, r, n are co-prime and so $r \in U(n)$

Now we have $x = qn + r$, where $1 \leq r < n$

$\Rightarrow \quad ax = aqn + ar$

$\Rightarrow \quad ax + ny = aqn + ar + ny$

$\Rightarrow \quad 1 = aqn + ar + ny$

or $\quad ar = 1 + (-aq - y)n$; i.e.; $a \otimes_n r = 1$.

Similarly $r \otimes_n a = 1$.

Therefore, $r = a^{-1}$.

Hence, $U(n)$ forms a group w.r.t $\otimes_n$ (multiplication modulo n).

Also, since $a \otimes_n b = b \otimes_n a$, for all $a, b \in U(n)$, we have that the group $U(n)$ is abelian.

This group is called **group of units**†

Remark: We have, $U(6) = \{1, 5\}$,

$U(7) = \{1, 2, 3, 4, 5, 6\}$, 7 is a prime number,

$U(8) = \{1, 3, 5, 7\}$,

$U(11) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, 11 is a prime number,

Therefore, in general, we have $U(p) = \{1, 2, 3, ..., p - 1\}$, p is a prime.

Problem 1.10 Show that the set $G = \{1, 2, ..., n - 1\}$ forms a group w.r.t. multiplication modulo n if and only if n is prime.

Solution Suppose G forms a group with respect to multiplication modulo n.

We show: n is prime.

Let, if possible, n is not prime.

Then, $n = rs$, where $1 < r, s < n$.

Now $1 < r < n$ gives that $r \in G$.

Also, since G is a group with respect to multiplication modulo n, we have r has inverse in G.

Therefore, there exists some $t \in G$ such that $r \otimes_n t = 1$

$\Rightarrow$ $rt = nq + 1$ which gives $rt = rsq + 1$.

$\Rightarrow$ $r(t - sq) = 1$

$\therefore$ $r \leq 1$, which is a contradiction as $r > 1$.

Hence, our assumption is wrong. Therefore, n must be prime.

Conversely, let n be prime p, then $G = \{1, 2, 3, ..., p - 1\}$

$= \{x \in \mathbb{Z} : 1 \leq x < p, \gcd(x, p) = 1\}$

$= U(p)$, which is a group.

Therefore, G is a group with respect to multiplication modulo p.

† Here units refer to elements with a multiplicative inverse, which in this case are exactly those co-prime to n

Remark:
Suppose in the set G, p is not prime. Then, there exists two integers a and b such that $1 < a \leq p - 1$, $1 < b \leq p - 1$ and $ab = p$. Now $a, b \in G$ such that $a \otimes_p b = 0$ and $0 \notin G$. Therefore, G is not closed w.r.t. multiplication modulo p. Thus, $(G, \otimes_p)$ is not a group.

Caution: If we include 0 in the set G, then also, for this composition, G will not be a group. The reason being, the inverse of 0 does not exist.

For example, the set $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4. Although 1 and 3 have inverses itself, the elements 0 and 2 do not.

Problem 1.11 Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

Solution We first construct the Cayley table for $\{1, 2, 3\}$ under multiplication modulo 4

Table 1.8: Cayley Table under multiplication modulo 4

$\otimes_4$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

The set $\{1, 2, 3\}$ is not a group because

(i) $2 \otimes_4 2 = 0$ does not belong to the set $\{1, 2, 3\}$

(ii) Inverse of the element 2 does not exist.

Now, consider the Cayley table of the set $S = \{1, 2, 3, 4\}$ under multiplication modulo 5

Table 1.9: Cayley Table under multiplication modulo 5

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The set S is closed under multiplication modulo 5 and also associativity holds. 1 is the identity element. Also, inverse of 1 is 1, 2 is 3, 3 is 2 and 4 is 4. Thus, S forms a group under multiplication modulo 5.

Problem 1.12 Show that for all integers $n \geq 1$, the set of complex roots of unity

$$\left\{ \cos\frac{k\cdot 2\pi}{n} + i \sin\frac{k\cdot 2\pi}{n} \,\middle|\, k = 0, 1, 2, ..., n-1 \right\}$$

is a group under multiplication.

Solution

We have, $\cos\dfrac{2k\pi}{n} + i \sin\dfrac{2k\pi}{n} = e^{i2k\pi/n}$

Then $G = \{1, e^{2\pi i/n}, e^{4\pi i/n}, e^{6\pi i/n}, ..., e^{2(n-1)\pi i/n}\} = \{1, \omega, \omega^2, \omega^3, ..., \omega^{n-1}\}$,

where $\omega = e^{2\pi i/n}$ and $\omega^n = 1$.

(i) **Closure:** Let $a, b \in G$, then $a^n = 1$ and $b^n = 1$.

Now $(ab)^n = a^n b^n = 1.1 = 1, \quad \therefore \quad ab \in G$

Thus, G is closed with respect to multiplication.

(ii) **Associativity:** The elements of G are all complex numbers and the multiplication of complex numbers is associative.

(iii) **Identity:** We have $1 \in G$ and $1.a = a = a.1 \ \forall a \in G$. Therefore, 1 is the identity of G.

(iv) **Inverse:** Let ω^k, $1 \leq k \leq n-1$ be any element of G, then ω^{n-k} is also an element of G and $\omega^{n-k} \cdot \omega^k = \omega^n = 1 = \omega^k \cdot \omega^{n-k}$

Thus ω^{n-k} is the inverse of ω^k.

Further, the multiplication of complex numbers is commutative. Therefore G is a finite abelian group with respect to multiplication.

Remark: We have $(1)^{1/n} = (1 + 0i)^{1/n} = (\cos 0 + i \sin 0)^{1/n}$

$= (\cos 2k\pi + i \sin 2k\pi)^{1/n}$, where k is any integer

$= \left(\cos\dfrac{2k\pi}{n} + i \sin\dfrac{2k\pi}{n} \right)$, by De' Moivre's Theorem

$= e^{i2k\pi/n}$.

Putting $k = 0, 1, 2, ..., n-1$, we get the n, n^{th} roots of unity.

Therefore the set of n, n^{th} roots of unity is a finite abelian group with respect to multiplication.

PROBLEM 1.13 Show that $SL(2, F)^{\dagger} = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in F, |A| = 1 \right\}$ is a non-abelian group under matrix multiplication.

Here F can be $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Z}_n$.

SOLUTION Let $A, B \in SL(2, F)$, then $|A| = 1$ and $|B| = 1$.

Since $|AB| = |A| \cdot |B| = 1.1 = 1$, therefore $AB \in SL(2, F)$.

Thus, $SL(2, F)$ is closed under matrix multiplication.

We know that matrix multiplication is always associative. Thus, associativity holds.

Also, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2, F)$ is the identity element.

Inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, F)$ is $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in SL(2, F)$.

Also, matrix multiplication is not commutative in general.

Therefore, $SL(2, F)$ is a non-abelian group under matrix multiplication.

PROBLEM 1.14 Give an example of group elements a and b with the property that $a^{-1} ba \neq a$.

SOLUTION Let us take the group as the set of matrices in $SL(2, \mathbb{R})$.

Let $a = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in SL(2, R)$ and $b = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in SL(2, R)$.

$\therefore \quad |a| = 1$ and $|b| = 1$.

The inverse of a, i.e., $a^{-1} = \begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix}$.

Now

$$a^{-1} ba = \begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

$$= \begin{bmatrix} a_2 d_1 - b_1 c_2 & d_1 b_2 - b_1 d_2 \\ -c_1 a_2 + a_1 c_2 & -c_1 b_2 + a_1 d_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 d_1 - a_1 b_1 c_2 + d_1 b_2 c_1 - b_1 d_2 c_1 & a_2 d_1 b_1 - b_1 c_2 b_1 + d_1 d_2 d_1 - b_1 d_2 d_1 \\ -c_1 a_2 a_1 + a_1 c_2 a_1 - c_1 b_2 c_1 + a_1 d_2 c_1 & -c_1 a_2 b_1 + a_1 c_2 b_1 - c_1 b_2 d_1 + a_1 d_2 d_1 \end{bmatrix}$$

$$\neq \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

$\therefore \quad a^{-1} ba \neq a.$

† This group is called the special linear group of 2×2 matrices over F.

Problem 1.15 Show that the set $\mathbb{Q}\backslash\{0\}$ of rational numbers form an abelian group under the binary operation $*$ defined by

$$a * b = a + b + ab \;\forall\; a, b \in \mathbb{Q}\backslash\{0\}$$

Solution Closure follows as $a * b = a + b + ab \in \mathbb{Q}\backslash\{0\} \;\forall\; a, b \in \mathbb{Q}\backslash\{0\}$

$$\begin{aligned}(a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc.\end{aligned}$$

Similarly, $a * (b * c) = a + b + c + ab + ac + bc + abc$

Therefore, associativity holds.

0 is the identity and $-\dfrac{a}{a+1}$ is the inverse of any element $a \in \mathbb{Q}\backslash\{0\}$.

Also, $a * b = a + b + ab = b + a + ba = b * a$

Therefore, $(\mathbb{Q}\backslash\{0\}, *)$ is an abelian group.

Problem 1.16 Let $G = \{(a, b) : a, b \in \mathbb{R}, a \neq 0\}$. Define $*$ on G by

$$(a, b) * (c, d) = (ac, bc + d)$$

Show that $(G, *)$ is a non abelian group.

Solution Closure follows as $a, c \neq 0 \;\Rightarrow\; ac \neq 0$

Let $x = (a, b), y = (c, d)$ and $z = (e, f) \in G$

Then,
$$\begin{aligned}(x * y) * z &= (ac, bc + d) * (e, f) \\ &= ((ac)e, (bc + d)e + f) = (a(ce), b(ce) + de + f) \\ &= (a, b) * (ce, de + f) = (a, b) * \{(c, d) * (e, f)\} \\ &= x * (y * z)\end{aligned}$$

Therefore, associativity holds.

$(1, 0)$ is the identity in G and $(a^{-1}, -ba^{-1})$ is the inverse of any element $(a, b) \in G$.

Therefore, $(G, *)$ is a group

G is not abelian as

$$(1, 2) * (2, 3) = (2, 2.2 + 3) = (2, 7)$$
$$(2, 3) * (1, 2) = (2, 3.1 + 2) = (2, 5).$$

Problem 1.17 Let $G = \{(a, b) : a, b \in R$, not both zero$\}$. Define $*$ on G by

$$(a, b) * (c, d) = (ac - bd, ad + bc)$$

Show that $(G, *)$ is an abelian group.

SOLUTION Closure follows as $ac - bd$, $ad + bc$ are not both zero.

Let $x = (a, b)$, $y = (c, d)$ and $z = (e, f) \in G$

Then, $(x * y) * z = (ac - bd, ad + bc) * (e, f)$

$= ((ac - bd)e - (ad + bc) f), (ac - bd)f + (ad + bc)e)$

$= (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df))$

$= (a, b) * (ce - df, cf + de)$

$= x * (y * z)$

Therefore, associativity holds.

$(1, 0)$ is the identity in G and $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is the inverse of any element $(a, b) \in G$.

Also, $(a, b) * (c, d) = (ac - bd, ad + bc) = (ca - db, cb + da)$

$= (c, d) * (a, b)$

Therefore, $(G, *)$ is an abelian group.

PROBLEM 1.18 Let $G = \{2^n : n \in Z\}$. Prove that G forms an abelian group under usual multiplication.

Proof: For any 2^m, $2^n \in G$, $2^m \cdot 2^n = 2^{m+n} \in G$.

Thus closure holds.

Since multiplication of rationals is associative, therefore associativity holds.

$1 = 2^0 \in G$ is the identity.

For any $2^m \in G$, as $2^{-m} \in G$ and $2^m \cdot 2^{-m} = 2^0 = 1$,

We find each element of G has inverse.

Thus, G is a group.

Commutativity is obvious.

PROBLEM 1.19 Prove that the set $\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) | a_1, a_2, \ldots, a_n \in \mathbb{R}\}$ forms a group under component-wise addition, i.e., $(a_1, a_2, \ldots a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$.

(i) Closure: For $(a_1, a_2, \ldots a_n)$, $(b_1, b_2, \ldots, b_n) \in \mathbb{R}^n$, we have

$(a_1, a_2, \ldots a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \in \mathbb{R}^n$,

as addition in $\mathbb{R}$ is a binary operation.

$\therefore$ $\mathbb{R}^n$ is closed under component-wise addition.

(ii) Associativity:

For $(a_1, a_2, \ldots a_n), (b_1, b_2, \ldots, b_n), (c_1, c_2, \ldots, c_n) \in \mathbb{R}^n$, we have

$$\begin{aligned}((a_1, a_2, \ldots a_n) + (b_1, b_2, \ldots, b_n)) + (c_1, c_2, \ldots, c_n) \\ &= (a_1 + b_1, a_2 + b_2, \ldots a_n + b_n) + (c_1, c_2, \ldots, c_n) \\ &= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2, \ldots, (a_n + b_n) + c_n) \\ &= (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), \ldots, a_n + (b_n + c_n)) \\ &= (a_1, a_2, \ldots a_n) + (b_1 + c_1, b_2 + c_2, \ldots, b_n + c_n) \\ &= (a_1, a_2, \ldots, a_n) + ((b_1, b_2, \ldots, b_n) + (c_1, c_2, \ldots, c_n))\end{aligned}$$

$\therefore$ Component-wise addition in $\mathbb{R}^n$ is associative.

(iii) Identity: $(0, 0, \ldots, 0) \in \mathbb{R}^n$ is the identity as

$$\begin{aligned}(a_1, a_2, \ldots, a_n) + (0, 0, \ldots, 0) &= (a_1, a_2, \ldots, a_n) \\ &= (0, 0, \ldots, 0) + (a_1, a_2, \ldots, a_n) \; \forall (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n\end{aligned}$$

(iv) Inverse: $\forall (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n \; \exists \; (-a_1, -a_2, \ldots, -a_n) \in \mathbb{R}^n \ni$

$$\begin{aligned}(a_1, a_2, \ldots, a_n) + (-a_1, -a_2, \ldots, -a_n) &= (0, 0, \ldots, 0) \\ &= (-a_1, -a_2, \ldots, -a_n) + (a_1, a_2, \ldots, a_n)\end{aligned}$$

$\therefore$ $(-a_1, -a_2, \ldots, -a_n) \in \mathbb{R}^n$ is the inverse of $(a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$

Hence $\mathbb{R}^n$ is a group under component-wise addition.

Problem 1.20 For a fixed point (a, b) in $\mathbb{R}^2$, define $T_{a,b} : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$T_{a,b}(x, y) = (x + a, y + b).$$

Show that the set $G = T(\mathbb{R}^2) = \{T_{a,b} : a, b \in \mathbb{R}\}$ is a group under function composition.

Solution Let $T_{a,b}, T_{c,d} \in T(\mathbb{R}^2) = G$

Then, $T_{a,b}\, T_{c,d}(x, y) = T_{a,b}(x + c, y + d) = (x + c + a, y + d + b)$

$$= T_{a+c,b+d}(x, y) \in T(\mathbb{R}^2)$$

$\therefore$ $T(\mathbb{R}^2)$ is closed.

Also function composition is always associative. Therefore, associativity holds in G.

The element $T_{0,0} \in T(\mathbb{R}^2)$ is the identity as $T_{a,b}\, T_{0,0} = T_{a,b} = T_{0,0}\, T_{a,b}$.

The inverse of $T_{a,b} \in T(\mathbb{R}^2)$ is $T_{-a,-b} \in T(\mathbb{R}^2)$.

Also $T(\mathbb{R}^2)$ is abelian.

Therefore $T(\mathbb{R}^2)$ is an abelian group under function composition.

The elements of $T(\mathbb{R}^2)$ are called translations.

Problem 1.21 Prove that the set $G = \{0, 1, 2, 3, 4, 5\}$ is a finite abelian group of order 6 with respect to addition modulo 6.

Solution The Cayley table for G is

Table 1.10: Cayley Table under addition modulo 6

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

We see that all the entries in the composition table are elements of the set G. Therefore, G is closed with respect to addition modulo 6.

Associativity: If $a, b, c \in G$, and if $a \oplus_6 b = d$, then $(a \oplus_6 b) \oplus_6 c = d \oplus_6 c = e$(say)

$$a + b = 6q + d \quad \text{and} \quad d + c = 6q_1 + e.$$

This gives $$a + b + c = 6(q + q_1) + e,\ 0 \le e < 6$$

Now, let $b \oplus_6 c = f$. Then $a \oplus_6 (b \oplus_6 c) = a \oplus_6 f = g$ (say).

$\Rightarrow$ $$a + b + c = 6(q_2 + q_3) + g,\ 0 \le g < 6\,.$$

Since e and g are remainders obtained by dividing $a + b + c$ by 6, therefore $e = g$.

Thus, $$(a \oplus_6 b) \oplus_6 c = a \oplus_6 (b \oplus_6 c), \quad \forall a, b, c \in G.$$

Identity: Since $a \oplus_6 0 = a = 0 \oplus_6 a, \quad \forall a \in G$, we have that 0 is the identity of G.

Inverse: From the table, we see that the inverse of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.

The composition is commutative as the corresponding rows and columns in the composition table are identical.

The number of elements in the set G is 6. Therefore, $(G, \oplus_6)$ is a finite abelian group.

Problem 1.22 Show that the set $G = GL(2, \mathbb{Z}_5)$ is a finite non-abelian group with respect to multiplication modulo 5.

Solution We have

$$G = GL(2, \mathbb{Z}_5) = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}_5, \det A \neq 0 \right\}$$

Since entries belong to $\mathbb{Z}_5$, therefore, modulo 5 arithmetic is used in all calculations.

(i) **Closure:** Let $A, B \in G$ then $|A|, |B| \neq 0$.

Then, AB is a 2×2 matrix such that $|AB| = |A|\,|B| \neq 0$. Also, the entries are from $\mathbb{Z}_5$. Therefore $AB \in G$.

For example:

If $A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$, then $|A| = 12 - 16 = -4 \equiv 1 \pmod 5$,

$B = \begin{bmatrix} 0 & 3 \\ 3 & 4 \end{bmatrix}$, then $|B| = 0 - 9 = -9 \equiv 1 \pmod 5$

$$AB = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}\begin{bmatrix} 0 & 3 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 12 & 25 \\ 12 & 28 \end{bmatrix} \equiv \begin{bmatrix} 2 & 0 \\ 2 & 3 \end{bmatrix}$$

$|AB| = 6 - 0 = 6 \equiv 1 \pmod 5$. $\therefore$ $AB \in G$.

(ii) **Associativity:** Clearly $(AB)C = A(BC)$, $\forall A, B, C \in$ G (as matrix multiplication is always associative).

(iii) **Identity:** There exist $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ such that $AI = A = IA$, for all $A \in G$.

(iv) **Inverse:** For any $A \in G$, we have $|A| \neq 0$.

Since $(\mathbb{Z}_5^*, \otimes_5)$ is a group so that $|A|$ has multiplicative inverse in $\mathbb{Z}_5^*$, say b. Here, $\mathbb{Z}_5^* = \mathbb{Z}_5 - \{0\}$.

Now, $A \cdot Adj\ A = |A|I$

$\Rightarrow$ $bA \cdot Adj\ A = b|A|I = I$ ($\because$ $b|A| = 1$)

$\Rightarrow$ $A(bAdj\ A) = I \Rightarrow AB = I$, where $B = b\ Adj\ A$

Similarly, $BA = I$, $\therefore$ $A^{-1} = B \in G$.

For example:

Consider $A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix} \in G$. Then, $A^{-1} = \begin{bmatrix} 4 & -4 \\ -4 & 3 \end{bmatrix} \equiv \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$

$|A^{-1}| = 12 - 1 = 11 \equiv 1 \pmod 5$. $\therefore$ $A^{-1} \in G$.

Clearly, it can be seen that $\forall A \in G, \exists\, A^{-1} \in G$ such that $AA^{-1} = I = A^{-1}A$.

(v) **Commutativity:** $AB \neq BA$, for all $A, B \in G$

($\because$ Matrix multiplication is not commutative in general)

Also, G is finite as for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$, the entries $a, b, c, d \in \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

Therefore, $GL(2, \mathbb{Z}_5)$ is a finite non-abelian group with respect to multiplication.

Note that:

- Generally, if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $A^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$
- Division by $ad - bc$ has to be interpreted as multiplication by the inverse of $ad - bc$ (modulo n).

ILLUSTRATION: $G = GL(2, \mathbb{Z}_7)$ w.r.t. multiplication, and $A = \begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$, then

$$|A| = 12 - 30 = -18 \equiv 3 \pmod 7$$

Also, inverse of 3 is 5 in the composition table for $\mathbb{Z}_7$.

$$\therefore \quad A^{-1} \equiv \frac{1}{3}\begin{bmatrix} 3 & -5 \\ -6 & 4 \end{bmatrix} \equiv \frac{1}{3}\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix} \equiv \begin{bmatrix} 3.5 & 2.5 \\ 1.5 & 4.5 \end{bmatrix} = \begin{bmatrix} 15 & 10 \\ 5 & 20 \end{bmatrix} \equiv \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix}.$$

PROBLEM 1.23 Find the inverse of $A = \begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $\mathbb{Z}_{11}$.

SOLUTION We have $\mathbb{Z}_{11} = \{0, 1, 2, 3, \ldots, 10\}$

[negative of any number = that number + 11, $\frac{1}{a}$ is determined by multiplying a with $b \in \mathbb{Z}_{11}$ such that ab when divided by 11 has 1 as the remainder. Then $b = 1/a$]

$$|A| = 10 - 18 = -8 \equiv 3 \bmod(11).$$

Also $$\text{adj } A = \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} \equiv \begin{pmatrix} 5 & 5 \\ 8 & 2 \end{pmatrix}.$$

Therefore $$A^{-1} = \frac{1}{|A|} adj\ A \equiv \frac{1}{3}\begin{pmatrix} 5 & 5 \\ 8 & 2 \end{pmatrix} \equiv 4\begin{pmatrix} 5 & 5 \\ 8 & 2 \end{pmatrix} = \begin{pmatrix} 20 & 20 \\ 32 & 8 \end{pmatrix} \equiv \begin{pmatrix} 9 & 9 \\ 10 & 8 \end{pmatrix}.$$

PROBLEM 1.24 Show that the set $G = \{f_1, f_2, f_3, f_4\}$, where

$$f_1(x) = x, f_2(x) = -x, f_3(x) = \frac{1}{x}, f_4(x) = -\frac{1}{x} \quad \forall x \in R - \{0\}$$

is a group with respect to composition of functions.

SOLUTION The Cayley table for G is as follows:

Table 1.11: Cayley Table of G

o	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Clearly, from the Cayley table, (G, o) is an abelian group.

The identity element is f_1 and $f_i^{-1} = f_i$ for $i = 1, 2, 3, 4$.

PROBLEM 1.25 Show that the set $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, where

$$f_1(x) = x, f_2(x) = 1 - x, f_3(x) = \frac{1}{x}, f_4(x) = \frac{1}{1-x},$$

$$f_5(x) = \frac{x-1}{x}, f_6(x) = \frac{x}{1-x} \quad \forall x \in R - \{0\}$$

is a group with respect to composition of functions.

SOLUTION The Cayley table for G is as follows:

Table 1.12: Cayley Table of G

o	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

Clearly, from the Cayley table, (G, o) is a group.

f_1 is the identity element and the inverse elements of $f_1, f_2, f_3, f_4, f_5, f_6$ are $f_1, f_2, f_3, f_5, f_4, f_6$ respectively. Since, $f_3 \, o \, f_5 \neq f_5 \, o \, f_3$, therefore G is non-abelian.

1.3 ELEMENTARY PROPERTIES OF GROUPS

In sections 1.1 and 1.2, we have given a variety of examples of groups. In these examples, we observed that identity element was unique and each element had a unique inverse. This was not by chance. We shall prove in the next theorem that identity element in a group is unique and each element has a unique inverse. In

fact we show that certain formal properties which follow from the group axioms hold in any group.

THEOREM 1.1: In a group G, prove that

1. Identity element is unique.
2. Inverse of each $a \in G$ is unique.
3. $(a^{-1})^{-1} = a$, $\forall a \in G$, where a^{-1} stands for inverse of a, i.e., a is the inverse of the inverse of a.
4. $(ab)^{-1} = b^{-1} a^{-1}$, $\forall a, b \in G$, i.e., the inverse of a product is the product of the inverses in reverse order.
5. $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}$, for $a_1, a_2, \ldots, a_n$ in G; a generalization of (4) to the product of n terms.
6. $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$ $\forall a, b, c \in G$.

These are known as **cancellation laws**.

The most basic rule of calculation in groups is the cancellation law, which allows us to cancel the factor a in the equations $ab = ac$ and $ba = ca$.

Proof:

1. To prove that identity element is unique. Let us suppose e and e' be two elements of G which act as identity.

   Then, since $e \in G$ and e' is identity, therefore we have

   $$e'e = ee' = e \qquad \ldots(1)$$

   and as $e' \in G$ and e is identity, therefore

   $$e'e = ee' = e' \qquad \ldots(2)$$

   From (1) and (2), we get that $e = e'$, which establishes the uniqueness of the identity element in a group.
2. We show that inverse of each $a \in G$ is unique.

   Let $a \in G$ be any element and let a' and a'' be two inverse elements of a, then $aa' = a'a = e$ and $aa'' = a''a = e$

   To show: $a' = a''$.

   Now, $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$, showing thereby that inverse of an element is unique.

   We shall denote inverse of a by a^{-1}.
3. To show: $(a^{-1})^{-1} = a$, $\forall a \in G$, where a^{-1} stands for inverse of a.

   Since a^{-1} is inverse of a, $\therefore aa^{-1} = a^{-1} a = e$ which also implies a is inverse of a^{-1}.

   Thus, $(a^{-1})^{-1} = a$.
4. To prove $(ab)^{-1} = b^{-1} a^{-1}$, $\forall a, b \in G$, we need to prove that $b^{-1} a^{-1}$ is inverse of ab for which we need to show that

   $$(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e.$$

Now, $(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e.$

Similarly $(b^{-1}\, a^{-1})\ (ab) = e$ and thus the result follows.

5. To show: $(a_1a_2 \ldots a_n)^{-1} = a_n^{-1}\, a_{n-1}^{-1} \ldots a_1^{-1}$ for $a_1, a_2, \ldots, a_n$ in G

We prove the result by induction on n. Clearly the result holds for $n = 1$.

Suppose that the result holds for $n = k$, i.e.,

$$(a_1\, a_2 \ldots a_k)^{-1} = a_k^{-1}\, a_{k-1}^{-1} \ldots a_1^{-1} \qquad \ldots(i)$$

Now, $(a_1\, a_2 \ldots a_{k+1})^{-1} = ((a_1\, a_2 \ldots a_k)\, a_{k+1})^{-1}$

$= (a_{k+1})^{-1}\ (a_1\, a_2 \ldots a_k)^{-1}$ [Using (4)]

$= (a_{k+1})^{-1}\ (a_k^{-1}\, a_{k-1}^{-1} \ldots a_1^{-1})$ [Using (i)]

$= a_{k+1}^{-1}\, a_k^{-1} \ldots a_1^{-1}$

Hence, the result holds for $n = k + 1$.

Thus, by induction, the result holds for all natural numbers n.

6. To prove the cancellation laws:

$$ab = ac \ \Rightarrow\ b = c \quad \text{and} \quad ba = ca \ \Rightarrow\ b = c\ \forall a, b, c \in G.$$

Let $ab = ac$, then $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c.$

Thus, $ab = ac \Rightarrow b = c,$ which is called the **left cancellation law**.

Now let $ba = ca$, then

$$b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)a^{-1} = c(aa^{-1}) = ce = c.$$

Thus $ba = ca \Rightarrow b = c,$ which is called the **right cancellation law.**

Remarks:

- In a semi-group, the cancellation laws may not hold.

  Consider the following example:

  Let S be the set of all 2×2 matrices over integers.

  We know that S is a semi-group under multiplication.

  Now, for $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ and $C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in S$, we note that

  $AB = AC$ but $B \neq C$.

- There are semi-groups which are not groups but they satisfy cancellation laws.

  Consider the set of positive integers. We know that it is a semi-group under addition.

  Clearly, for any three positive integers a, b, c, we have

  $a + b = a + c \ \Rightarrow\ b = c$ and $b + a = c + a \ \Rightarrow\ b = c.$

  So, the cancellation laws hold. But this semi-group is not a group (why ?).

Any finite semi-group, in which both the cancellation laws hold, forms a group.

We shall prove this in the following problem.

PROBLEM 1.26 A finite semi-group S, in which both the cancellation laws hold, is a group.

SOLUTION Let S be a finite semi-group in which both the cancellation laws hold.

Let $S = \{a_1, a_2, \ldots, a_n\}$. ...(1)

Let a be any element of S. Then a is one of the $a_i's$ for $1 \le i \le n$.

By closure in S, $aa_1, aa_2, \ldots, aa_n \in S$ ...(2)

and they are all distinct, for if $aa_i = aa_j$ for some $i \ne j$, then by left cancellation law, $a_i = a_j$, which is a contradiction. Hence elements in (2) are all the elements in (1), in possibly some other order.

Similarly, using right cancellation law, it follows that

$$a_1a, a_2a, \ldots, a_na \quad \ldots(3)$$

are all distinct elements of S.

Let a_i, $1 \le i \le n$, be any element of S. Then a_i must be one of the elements listed in (3).

Let $a_i = a_j a$ for some, $1 \le j \le n$. ...(4)

Also, since $a \in S$, then as argued above

$a = a_k a$ for some k, $1 \le k \le n$. ...(5)

Consider $a_i a = a_i(a_k a)$ by (5)

$= (a_i a_k)a$ [As S is a semi-group, using associativity]

$\Rightarrow$ $a_i = a_i a_k$ [By right cancellation law]

Thus, $a_i = a_i a_k$ for all i, $1 \le i \le n$ ...(6)

Similarly, by taking a_i to be one of the elements listed in (2), we have

$a_i = a_t a_i$ for all i, $1 \le i \le n$ and for some t, $1 \le t \le n$ ...(7)

In particular, $a_k = a_t a_k$ [Taking $i = k$ in (7)]

$= a_t$ [Taking $i = t$ in (6)]

$\therefore$ $a_k = a_t$. ...(8)

Using (8) in (6) and (7), we get

$$a_i a_k = a_k a_i = a_i \quad \text{for all} \quad i = 1, 2, \ldots, n$$

Hence a_k is the identity element in S.

Let us write e for a_k.

Since $e \in S$, therefore by (2) and (3),

$e = aa_r$ for some r, $1 \le r \le n$ ...(9)

and $e = a_s a$ for some s, $1 \le s \le n$ ...(10)

Now, $a_r = ea_r$, since e is the identity in S

$= (a_s a)a_r$ by (10)

$= a_s(aa_r) = a_s e$ by (9)

$= a_s$, since e is the identity in S

Using $a_r = a_s$ in (9) and (10), we get

$$aa_r = a_r a = e$$

$$\Rightarrow \quad a^{-1} = a_r \in S$$

Consequently, every element in S has its inverse in S.

Hence S is a group.

Remark: The above result may not be true if only one of the cancellation laws holds. This is shown by the following example.

Let G be a finite set having at least two elements.

Given $a, b \in G$, define $a \cdot b = b$.

Clearly G is a finite semi-group but is not a group (why ?).

Let $a, b, c \in G$.

Since $a \cdot b = a \cdot c \Rightarrow b = c$, therefore left cancellation law holds.

Now, consider two distinct elements a, b in G.

Then, $a \cdot b = b, b \cdot b = b$.

Consequently, $b \cdot b = a \cdot b$ but $a \neq b$.

So, G does not satisfy right cancellation law.

Thus, we have the following result:

A finite semi-group G is a group if and only if G satisfies both the cancellation laws.

The following are the same conventions that are used in elementary algebra, and they lead to the same familiar laws of exponents.

Definition 1.9: Let G be a group and a be any element of G. We define **integral powers** of a as follows:

(i) $a^0 = e$

(ii) $a^m = aaa \ldots a$ (m times) $\forall\ m \in N$

(iii) $a^{-m} = (a^{-1})^m$, $m \in N$

PROBLEM 1.27 Let $a \in G$. Show that $a^{n+m} = a^n\, a^m$, where m and n are any integers.

SOLUTION Let $n = 1$ and $m = 1$, then LHS $= a^2 = aa$ and RHS $= aa$

$\therefore$ $P(n)$ is true for $n = 1$.

Let $P(k)$ be true, i.e., for k_1 and k_2,

$$a^{k_1+k_2} = a^{k_1}\, a^{k_2}.$$

To show: $P(k + 1)$ is true, i.e., for k_1 and k_2,

$$a^{(1+k_1)+(1+k_2)} = a^{1+k_1}\, a^{1+k_2}$$

$$\text{LHS} = a^{(1+k_1)+(1+k_2)} = a^{2+k_1+k_2} = a^2 a^{k_1+k_2} = a^2\, a^{k_1}\, a^{k_2} = a^{1+k_1}\, a^{1+k_2} = \text{RHS}$$

$\therefore$ $P(k + 1)$ is true, whenever $P(k)$ is true

$\therefore$ $a^{n+m} = a^n\, a^m$.

PROBLEM 1.28 Let $a \in G$. Show that $(a^n)^m = a^{nm}$, for integers m and n.

SOLUTION Let $n = 1$ and $m = 1$.
Then we have LHS $= (a^1)^1 = a$ and RHS $= a^{1.1} = a$.

Thus LHS = RHS, therefore $P(n)$ is true for $n = 1$.

Let $P(k)$ be true, i.e., for k_1 and k_2,

$$(a^{k_1})^{k_2} = a^{k_1 k_2}$$

To show: $P(k + 1)$ is true, i.e., for k_1 and k_2, $(a^{1+k_1})^{1+k_2} = a^{(1+k_1)(1+k_2)}$.

$$(a^{1+k_1})^{1+k_2} = (a\, a^{k_1})^{1+k_2} = (a^1)^{1+k_2}\, (a^{k_1})^{1+k_2}$$

$$= a^{1+k_2}\, a^{k_1+k_1k_2} = (a)^{1+k_1+k_2+k_1k_2} = (a)^{(1+k_1)(1+k_2)}$$

$\therefore$ $P(k + 1)$ is true whenever $P(k)$ is true. Hence $(a^n)^m = a^{nm}$.

PROBLEM 1.29 If in a group G, $a^2 = e$, $\forall a \in G$, then show that $ab = ba$, $\forall a, b \in G$, i.e., the group G is abelian.

SOLUTION We have,

$$a^2 = e \;\Rightarrow\; a^{-1} a^2 = a^{-1} e \;\Rightarrow\; (a^{-1}a)\, a = a^{-1} \;\Rightarrow ea = a^{-1} \;\Rightarrow\; a = a^{-1}.$$

Since for all $a, b \in G$, we have $ab \in G$, therefore, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

Therefore the group G is abelian.

Remark: We can have another problem:
If $a = a^{-1}$, $\forall\ a \in G$, show that the group G is abelian, i.e., if in a group G, every element is the inverse of itself, then G is abelian.

Problem 1.30 If in a group G, $(ab)^2 = a^2b^2$, $\forall\ a, b \in G$, then show that $ab = ba$, i.e., G is abelian and conversely.

Solution Given: $(ab)^2 = a^2b^2$

$\Rightarrow$ $(ab)\ (ab) = (aa)\ (bb)$

$\Rightarrow$ $a(ba)\ b = a(ab)\ b$ (as G is a group, so associativity holds)

By left and right cancellation laws, we get $ba = ab$. Therefore, G is abelian.

Conversely: Let $ba = ab,\ \forall\ a, b \in G$

Then $(ab)^2 = (ab)\ (ab) = a(ba)b$ (as G is associative)

$= a(ab)b$ (as G is abelian)

$= (aa)\ (bb)$ (as associativity holds in G)

$= a^2\ b^2$.

Problem 1.31 If in a group G, $ab = ba\ \forall\ a, b \in G$, i.e., if the group G is abelian, show that $(ab)^n = a^nb^n$, where n is any integer.

Solution

Case I: When $n = 0$, the result is obvious.

Case II: When $n > 0$, we shall prove the result by induction on n.

For $n = 1$, LHS $= (ab)^1 = ab = a^1b^1 =$ RHS.

Suppose the result is true for $n = k$. Then $(ab)^k = a^kb^k$ …(1)

Now, $(ab)^{k+1} = (ab)^k\ (ab) = (a^kb^k)\ (ab)$ (using (1))

$= a^k(b^ka)\ b = a^k(ab^k)b$

(as G is abelian, $\therefore\ ab^k = b^k\ a$)

$= (a^ka)\ (b^kb) = a^{k+1}b^{k+1}$

This gives that the result is true for $n = k + 1$ also.

Thus, by induction, $(ab)^n = a^n\ b^n$.

Case III: When $n < 0$, let $n = -m$, where m is a positive integer.

Then $(ab)^n = (ab)^{-m} = ((ab)^m)^{-1}\quad (a^mb^m)^{-1}$ (by case (II))

$= (b^ma^m)^{-1}$ ($\because\ ab = ba, \forall\ a, b \in G$)

$= (a^m)^{-1}(b^m)^{-1} = a^{-m}b^{-m} = a^nb^n$.

Thus $(ab)^n = a^nb^n$, where n is any integer.

Problem 1.32 If in a group G, $(ab)^n = a^n b^n$ for three consecutive integers n, and for all $a, b \in G$, show that G is abelian.

Solution Given:

$(ab)^n = a^n b^n$, $(ab)^{n+1} = a^{n+1}\, b^{n+1}$ and $(ab)^{n+2} = a^{n+2}\, b^{n+2}$ for all $a, b \in G$.

Then, we have $(ab)^{n+2} = (ab)^{n+1}(ab)$

$\Rightarrow$ $a^{n+2}\, b^{n+2} = (a^{n+1}b^{n+1})ab$ (given)

$\Rightarrow$ $a^{n+1}\, ab^{n+1}b = a^{n+1}\, b^{n+1}ab$

$\Rightarrow$ $ab^{n+1} = b^{n+1}a$ (by left and right cancellation laws)

$\Rightarrow$ $a^n(ab^{n+1}) = a^n(b^{n+1}\, a)$

$\Rightarrow$ $a^{n+1}\, b^{n+1} = a^n\, b^n(ba)$

$\Rightarrow$ $(ab)^{n+1} = (ab)^n\, ba$ (given)

$\Rightarrow$ $(ab)^n\, (ab) = (ab)^n\, ba$

$\Rightarrow$ $ab = ba$ (by left cancellation law)

$\Rightarrow$ G is abelian.

Remark: The conclusion of the above problem does not follow, if we assume the relation $(ab)^n = a^n\, b^n$ for just two consecutive integers.

Suppose $(ab)^i = a^i\, b^i$ for $i = n$ and $i = n + 1$.

We claim G is abelian if and only if $(ab)^{n+2} = a^{n+2}\, b^{n+2}$

Clearly, from the above problem, we have $(ab)^{n+2} = a^{n+2}\, b^{n+2} \Rightarrow G$ is abelian.

Also if G is abelian, then $(ab)^i = a^i\, b^i\ \forall\ i \in \mathbb{Z}$; in particular result holds for $i = n + 2$.

Thus G is abelian if and only if $(ab)^{n+2} = a^{n+2}\, b^{n+2}$.

So the result of the above problem might not follow, if we assume that $(ab)^i = a^i\, b^i$ for just two consecutive integers.

Problem 1.33 If a and b be any two elements of a group G, then prove that $(bab^{-1})^n = ba^n\, b^{-1}$ for any integer n.

Solution **Case I:** When $n = 0$, we have, $(bab^{-1})^0 = e$.

Also, $ba^0\, b^{-1} = beb^{-1} = bb^{-1} = e$

$\therefore$ $(bab^{-1})^0 = ba^0b^{-1}$.

Case II: When $n > 0$. Then

$(bab^{-1})^1 = bab^{-1} = ba^1b^{-1}$ $(\because\ a^1 = a)$

Thus, the result is true for $n = 1$.

Let the result be true for $n = k$, i.e.,

$$(bab^{-1})^k = ba^k b^{-1}.$$

Then
$$(bab^{-1})^{k+1} = (bab^{-1})^k\,(bab^{-1}) = (ba^k b^{-1})\,(bab^{-1})$$
$$= ba^k\,(b^{-1}b)ab^{-1}$$
$$= b(a^k\,a)b^{-1} = ba^{k+1}\,b^{-1}.$$

Therefore the result is true for $n = k + 1$ also.

Hence, by induction, the result is true for all $n > 0$.

Case III: When $n < 0$. Let $n = -m$, where $m > 0$. Then

$$(bab^{-1})^n = (bab^{-1})^{-m} = ((bab^{-1})^m)^{-1} = (ba^m b^{-1})^{-1}$$
$$= (b^{-1})^{-1}(a^m)^{-1}b^{-1} = ba^{-m}b^{-1} = ba^n b^{-1}.$$

Problem 1.34 Let G be a group such that $ab = ca$ gives $b = c, \forall a, b, c \in G$. Show that G is abelian.

Solution Since we have $a^{-1}\,a = e = aa^{-1}$ for all $a \in G$,

$\therefore \quad (a^{-1}\,a)\,b = b(aa^{-1})$ gives $a^{-1}\,(ab) = (ba)\,a^{-1}$.

Therefore, by the given hypothesis, $ab = ba$. Hence G is abelian.

Problem 1.35 Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}\,b^{-1}$ for all a, b in G.

Solution Let G be abelian, then $ab = ba, \quad \forall a, b \in G$.

Now, $\quad e = (ab)\,(ab)^{-1}$ or $(ab)^{-1}\,ab$

$\Rightarrow \quad eb^{-1} = (ab)^{-1}\,abb^{-1}$

$\Rightarrow \quad b^{-1} = (ab)^{-1}\,ae$

$\Rightarrow \quad b^{-1}a^{-1} = (ab)^{-1}\,aa^{-1}$

$\Rightarrow \quad b^{-1}\,a^{-1} = (ab)^{-1}$

$\Rightarrow \quad a^{-1}\,b^{-1} = (ab)^{-1}$ $\quad (\because\ G$ is abelian)

Conversely, given that $(ab)^{-1} = a^{-1}\,b^{-1} \quad \forall\ a, b \in G$

$\Rightarrow \quad (ab)\,(ab)^{-1} = (ab)\,(a^{-1}\,b^{-1})$

$\Rightarrow \quad e = (ab)\,(a^{-1}\,b^{-1})$

$\Rightarrow \quad a^{-1}\,e = (a^{-1}\,a)\,ba^{-1}b^{-1}$

$\Rightarrow \quad a^{-1}\,b = eba^{-1}\,b^{-1}\,b$

$\Rightarrow \quad aa^{-1}b = aba^{-1}$

$\Rightarrow \quad eb = aba^{-1}$

$\Rightarrow \quad ba = aba^{-1}\,a$

$\Rightarrow \quad ba = ab.$

Hence, G is abelian.

PROBLEM 1.36 Let $n > 2$. Show that $U(n)$ has at least two elements such that

$$x^2 = e \quad \text{where} \quad e = 1.$$

SOLUTION

$$1 \in U(n) \quad \text{and} \quad 1^2 = 1.$$

Let gcd $(n - 1, n) = d$. Then

$$d/n - 1, d/n \quad \Rightarrow \quad d/n - (n - 1) \quad \Rightarrow \quad d/1 \quad \Rightarrow \quad d = 1.$$

Therefore, $(n - 1) \in U(n)$ and

$$(n - 1)^2 = (n - 1) * (n - 1) = n^2 + 1 - 2n = n(n - 2) + 1 \equiv 1 \text{ (remainder)}$$

Also, since $n > 2$, we have that $n - 1 \neq 1$.

Thus there exist at least 2 elements in $U(n)$, $n > 2$ namely 1 and $n - 1$ such $1^2 = 1$ and $(n - 1)^2 = 1$.

PROBLEM 1.37 If $a_1, a_2, \ldots, a_n$ belong to a group, what is the inverse of $a_1 a_2 \ldots a_n$?

SOLUTION We have, $(a_1 a_2 \ldots a_n)(a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1})$

$$= a_1 a_2 \ldots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$$

$$= a_1 a_2 \ldots (a_{n-1} a_{n-1}^{-1}) \ldots a_2^{-1} a_1^{-1}$$

$$. \quad . \quad .$$

$$= a_1 (a_2 a_2^{-1}) a_1^{-1}$$

$$= a_1 e a_1^{-1} = e$$

Thus, $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$.

PROBLEM 1.38 Let a, b and c be elements of a group. Solve the equation $axb = c$ for x. Also, solve $a^{-1} xa = c$ for x.

SOLUTION We have $axb = c$.

Premultiplying both sides by a^{-1}, we have $a^{-1} axb = a^{-1} c$

$$\Rightarrow \quad exb = a^{-1} c$$

$$\Rightarrow \quad xbb^{-1} = a^{-1} cb^{-1} \quad \text{(postmultiplying both sides by } b^{-1})$$

$$\Rightarrow \quad xe = a^{-1} cb^{-1} \quad \text{or} \quad x = a^{-1} cb^{-1}.$$

Also we have $a^{-1} xa = c$

$$\Rightarrow \quad a^{-1} xaa^{-1} = ca^{-1}$$

$$\Rightarrow \quad a^{-1} xe = ca^{-1}$$

$$\Rightarrow \quad aa^{-1} x = aca^{-1}$$

$$\Rightarrow \quad ex = aca^{-1} \quad \text{or} \quad x = aca^{-1}$$

PROBLEM 1.39 Let G be a group and let $g \in G$. Define a function φ_g from G to G by $\varphi_g(x) = gxg^{-1}$, $\forall\, x \in G$. Show that φ_g is one to one and onto. Also, for $g, h \in G$, show that $\varphi_g \circ \varphi_h = \varphi_{gh}$.

SOLUTION To show that φ_g is one to one:

Let $\varphi_g(x) = \varphi_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow x = y$ (by cancellation laws)

Thus, φ_g is one-to-one.

Now let $y \in G$.

To show that φ_g is onto, we need to show that there exists some $x \in G$ such that

$$\varphi_g(x) = y, \quad \text{i.e.,} \quad gxg^{-1} = y, \quad \text{i.e.,} \quad x = g^{-1}yg.$$

$\therefore$ For any $y \in G$, there exists $x = g^{-1}yg \in G$ such that $\varphi_g(x) = y$.

Hence, φ_g is onto.

Now consider,

$$(\varphi_g \circ \varphi_h)(x) = \varphi_g(\varphi_h(x)) = \varphi_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(h^{-1}g^{-1})$$

Also, $\varphi_{gh}(x) = (gh)\,x(gh)^{-1} = (gh)\,x(h^{-1}g^{-1})$ $\quad (\because (ab)^{-1} = b^{-1}a^{-1})$

Therefore $\varphi_g \circ \varphi_h = \varphi_{gh}$.

PROBLEM 1.40 Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Also, show that the number of elements x of G such that $x^2 \neq e$ is even.

SOLUTION Let $x \in G$ be such that $x^2 \neq e$.

Then, $x \neq x^{-1}$ as if $x = x^{-1}$, then $x^2 = x^{-1}\,x = e$, which is not true.

Also, $x^2 \neq e \;\Rightarrow\; (x^2)^{-1} \neq e \;\Rightarrow\; (x^{-1})^2 \neq e$

Thus, elements $x \in G$ such that $x^2 \neq e$ occur in pairs as $\{x, x^{-1}\}$.

Hence the number of such elements is even.

Now, let $x \in G$ be such that $x^3 = e$, $x \neq e$.

We assert that $x^2 \in G$ is such that

1. $(x^2)^3 = e$
2. $x^2 \neq e$
3. $x \neq x^2$.

We now prove them one by one.

1. $x^3 = e \;\Rightarrow\; (x^3)^2 = e^2 = e \;\Rightarrow\; (x^2)^3 = e$.
2. If $x^2 = e$ then $x^3 = e \;\Rightarrow\; xx^2 = e \;\Rightarrow\; x = e$, which is not the case. Therefore, $x^2 \neq e$.
3. $x = x^2 \;\Rightarrow\; x = e$, a contradiction to our assumption, therefore $x \neq x^2$.

Thus elements $x \in G$ such that $x^3 = e$, $x \neq e$ occur in pairs as $\{x, x^2\}$.

Hence, the number of such elements is even.

Also $e^3 = e$, thus the number of elements x of G such that $x^3 = e$ is odd.

PROBLEM 1.41 Let $G = \{e, a, b, c\}$ with the property that $a^2 = b^2 = c^2 = e$ and the product of two distinct non-identity elements is the remaining non–identity element. Show that G forms a group under multiplication.

SOLUTION We have $G = \{e, a, b, c : a^2 = b^2 = c^2 = e\}$ such that

$$ab = ba = c, \quad ac = ca = b, \quad bc = cb = a$$

(i) **Closure:** The closure is established through the following composition table

Table 1.13: Cayley Table for G

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Clearly from the Cayley table given above, closure property holds.

(ii) **Associativity:** Clearly, $\forall a, b, c \in G$, we have $(ab)c = a(bc)$, therefore, associativity holds.

(iii) **Identity:** $e \in G$ is the identity element as

$$x \cdot e = x = e \cdot x \ \forall x \in G$$

(iv) **Inverse:** From the table we observe that the inverse of a, b, c are a, b, c itself.

Hence, $(G, .)$ is a group. Also $xy = yx$ for all $x, y \in G$. Thus, G is a finite abelian group. This group is called the **Klein Group** and is denoted by K_4.

PROBLEM 1.42 Prove that a semi-group S is a group if and only if it satisfies the following:

(i) There exists an element $e \in G$ such that $ea = a \ \forall \ a \in S$ (i.e. S has a left identify)

(ii) For all $a \in S$, there exist $a' \in S$ such that $a'a = e$. (i.e., each element in S has a left inverse)

SOLUTION Suppose a semi-group S satisfies the conditions (i) and (ii).

Let $a \in S$. Then by (ii) there exists some $a' \in S$ such that $a'a = e$ ...(1)

Again, for $a' \in S$, there exists $a'' \in S$ such that $a''a' = e$ ...(2)

Since $aa' \in S$, so by (i) $aa' = e(aa')$

$= (ea)a'$ (as S is a semi-group, by associativity)

$= ((a''a')a)a'$

$= (a''(a'a))a'$ (as S is a semi-group, by associativity)

$= (a''e)a'$ (by (1)]

$= a''(ea')$ (as S is a semi-group, by associativity)

$= a''a'$ (by condition (i))

$= e$ (by (2))

$\therefore \quad aa' = a'a = e$ ...(3)

Thus, each $a \in S$ has its inverse $a' \in S$.

Now, $ae = a(a'a)$ (by (1))

$= (aa')a$ (as S is a semi-group, by associativity)

$= ea$ (by (3))

$= a$ (by condition (i))

$\therefore \quad ae = ea = a \ \forall \ a \in S$

Thus, e is the identity in S.

Hence, S is a group.

Conversely, let S be a group.

Then, by definition of a group, the conditions (i) and (ii) immediately follow.

Remarks:

- In view of the above, in order to prove that a non-empty set G along with a binary composition, is a group, it is enough to prove that the operation is associative, the left identity exists and the left inverse of each element of G exists.
- We can also define a group with the help of right identity and right inverse only.
- However, we cannot define a group assuming the existence of left identity and right inverse or right identity and left inverse.

Problem 1.43 Show that in a group G, the equations $ax = b$ and $ya = b$ have unique solutions for all a, b in G.

Solution Since $a(a^{-1} b) = (aa^{-1})b = eb = b$, therefore $x = a^{-1} b$ is a solution of the equation $ax = b$ in G.

Similarly, $y = ba^{-1}$ is a solution of the equation $ya = b$ in G.

To show that the solution is unique, let us suppose that $x = x_1$ and $x = x_2$ be two solutions of the equation $ax = b$.

Then, $ax_1 = b$ and $ax_2 = b$. Therefore, $ax_1 = ax_2$.

By left cancellation law, we get $x_1 = x_2$.

Therefore, the solution is unique.

Problem 1.44 Show that in a semi-group G in which the equations $ax = b$ and $ya = b$ have solutions in G for every pair of elements a, b in G, is a group.

Solution We need to show that G has a right identity and every element of G has a right inverse.

Let $a \in G$. Consider the equation $ax = a$.

Since it has a solution in G, therefore there exists $e \in G \ni ae = a$.

Again, let $g \in G$. Since the equation $ya = g$ has a solution in G, therefore there exists some $h \in G \ni ha = g$.

Now, $ge = (ha)e = h(ae) = ha = g$.

Thus, $ge = g \ \forall \ g \in G$

Therefore, e is a right identity in G.

We now prove that every element in G has a right inverse.

Let $a \in G$. The equation $ax = e$ has a solution in G, say, a'.

Then, $aa' = e$.

Therefore, the element $a \in G$ has a right inverse $a' \in G$.

Thus, G is a semi-group with a right identity and each element has a right inverse.

Therefore, G is a group.

In view of the above two problems, we have the following problem:

Problem 1.45 Let G be a semi-group. Then, G forms a group if and only if the equations $ax = b$ and $ya = b$ are solvable in G, for all $a, b \in G$.

The above result gives a characterization of a group, so we may alternatively define a group as follows:

Definition: A non-empty set G together with a binary composition is called a group if it satisfies the following:

(i) $a(bc) = (ab)c$ for all $a, b, c \in G$

(ii) For any $a, b \in G$, the equations $ax = b$ and $ya = b$ have solutions in G.

Remark: If G is a semi-group and if we are given that for all $a, b \in G$ only the equation $ax = b$ has a solution in G, then G may not be a group.

Consider the following example:
Let G be any set having at least two elements.
Given $a, b \in G$, define $a \cdot b = b$.
Then, $a \cdot (b \cdot c) = a \cdot c = c$ and $(a \cdot b) \cdot c = b \cdot c = c$
Thus, the associativity holds.
Further, since $a \cdot b = b$, $x = b$ is a solution of the equation $ax = b$.
Consider two distinct elements a, b in G.
Then, $a \cdot b = b$, $b \cdot b = b$. Consequently, $b \cdot b = a \cdot b$ but $a \neq b$.
So, G does not satisfy cancellation laws.
Hence G is not a group.

Problem 1.46 If G is a finite group, show that there exists a positive integer k such that $a^k = e$ for all $a \in G$.

Solution Let $a \in G$.

Since G is a group, therefore by closure $a^2, a^3, a^4, \ldots$ are all elements of G. But G is finite, therefore, we must have $a^i = a^j$ for some integers i and j, $i > j$ (say).

$$\Rightarrow \quad a^i a^{-j} = a^j a^{-j}$$

$$\Rightarrow \quad a^{i-j} = a^0 = e$$

$\Rightarrow \quad a^k = e$, where $k = i - j > 0$

Hence, there exists a positive integer k such that $a^k = e$ for all $a \in G$.

Problem 1.47 (a) If the group G has three elements, show that it must be abelian.

(b) Do part (a) if G has four elements.

(c) Do part (a) if G has five elements.

Solution

(a) Let G be a group of order 3 and some $a, b \in G$ with $a \neq b$.

Case 1: Either of a or b equals to the identity element.

Suppose $a = e$, then

$$a \cdot b = e \cdot b = b = b \cdot e = b \cdot a.$$

Similarly if $b = e$, we have

$$a \cdot b = b \cdot a.$$

Thus if either a or b equals to e, we have $a \cdot b = b \cdot a$.

Case 2: Neither of a or b is identity element.

Consider $a \cdot b$. We have $a \cdot b \neq a$, otherwise it would mean $b = e$.

Similarly $a \cdot b \neq a$ as $a \neq e$.

Also, G has only three elements, so $a \cdot b$ has no option but to be equal to the identity element. Therefore,

$$a \cdot b = e.$$

A similar argument will show that $b \cdot a = e$.

Thus, $a \cdot b = b \cdot a$ in this case too.

So we have $a \cdot b = b \cdot a \ \forall\ a, b \in G$.

Hence, G is abelian for $o(G) = 3$.

(b) Again, let G be the group of order 4 and let some $a, b \in G$.

Case 1: Either of a, b equals to e.

In this case, clearly $a \cdot b = b \cdot a$.

Case 2: Neither of a, b equals to e.

Consider $a \cdot b$. Clearly, $a \cdot b \neq a$ and $a \cdot b \neq b$.

But since G has four elements, let $c \neq e$ be the fourth element.

So $a \cdot b$ has two options, either equals to e or equals to c.

If $a \cdot b = e$, then

$$a = b^{-1} \Rightarrow b \cdot a = b \cdot b^{-1} \Rightarrow b \cdot a = \text{e}.$$

Thus, $a \cdot b = b \cdot a = e$.

If $a \cdot b = c$, then consider $b \cdot a$. Clearly, $b \cdot a \neq a$ and $b \cdot a \neq b$.

So $b \cdot a$ has only two options, either $b \cdot a = e$ or $b \cdot a = c$.

But if $b \cdot a = e$, then it would imply $a \cdot b = e$, which is not true.

So $b \cdot a = c$ too. Thus

$$a \cdot b = b \cdot a = \text{c}.$$

Thus we have $a \cdot b = b \cdot a$ for all $a, b \in G$.

Hence, G is abelian for $o(G) = 4$.

(c) For this part, we have to make use of the material not presented till now in the book.

Since the order of G is prime, therefore it is cyclic.

But a cyclic group is abelian, so G must be abelian for order 5.

PROBLEM 1.48 Let G be the set of all real 2×2 matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ where $ad \neq 0$. Prove that G forms a group under matrix multiplication. Is G abelian?

SOLUTION We have G is closed under multiplication as

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} = \begin{bmatrix} aa' & ab' + bd' \\ 0 & dd' \end{bmatrix} \in G$$

Now, since $ad \neq 0$, therefore G forms a group under matrix multiplication with $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ as identity element and $\begin{bmatrix} 1/a & -b/ad \\ 0 & 1/d \end{bmatrix}$ as inverse element of $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$.

Finally, we have $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$

which implies $ab' + bd' = a'b + b'd$.

Since $ab' + bd' \neq a'b + b'd$ for all values of a, b, d, a', b', d', so G is not abelian.

Problem 1.49 Let G be the set of all real 2×2 matrices $\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$, where $a \neq 0$. Prove that G is an abelian group under matrix multiplication.

Solution It is easy to check that G is a group under multiplication.

Also, we have

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix} = \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = \begin{bmatrix} ba & 0 \\ 0 & b^{-1}a^{-1} \end{bmatrix}$$

Hence, G is abelian too.

Problem 1.50 Let $P(X)$ be the powerset of a set X. Consider the operation Δ(symmetric difference) on $P(X)$:

$\forall\ A, B \in P(X), A\Delta B = (A - B) \cup (B - A)$

Show that $(P(X), \Delta)$ is a commutative group.

Solution **Closure:** Let $A, B \in P(X)$

$\Rightarrow \quad A - B, B - A \in P(X)$

$\Rightarrow \quad (A - B) \cup (B - A) \in P(X)$, i.e., $A\Delta B \in P(X)$

Associativity: Using elementary set theory properties, it can be easily shown that associativity holds.

Existence of left identity:

The empty set φ is a subset of X. Therefore, $\varphi \in P(X)$.

If A be any member of $P(X)$, we have

$$\varphi\Delta A = (\varphi - A) \cup (A - \varphi) = \varphi \cup A = A.$$

Therefore, φ is the left identity.

Existence of left inverse:

We have $\forall\ A \in P(X), A\Delta A = (A - A) \cup (A - A) = \varphi \cup \varphi = \varphi$

which is a member of $P(X)$.

Therefore, every element of $P(X)$ is its own inverse,

Therefore, $(P(X), \Delta)$ is a group.

Commutativity: We have

$$\forall\ A, B \in P(X), A\Delta B = (A - B) \cup (B - A)$$

$$= (B - A) \cup (A - B) = B\Delta A$$

Therefore, $(P(X), \Delta)$ is a commutative group.

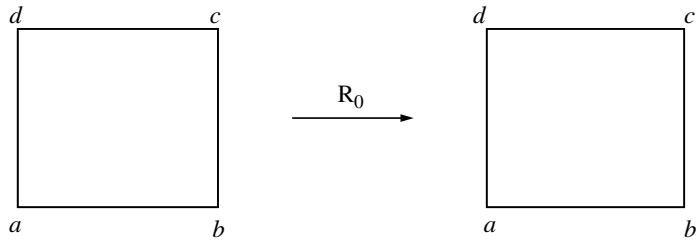
We now discuss yet another important class of groups called Dihedral Groups.

1.4 Dihedral Groups

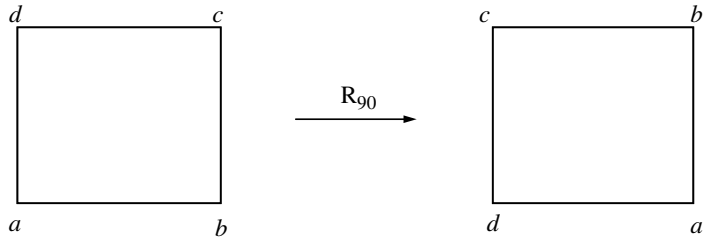
The dihedral groups are the group of symmetries of a regular n-sided polygon.

We have already discussed symmetries of an equilateral triangle in the beginning of the chapter. Let us now study the symmetries of a square by marking its corners as a, b, c, d and considering all the possible motions.

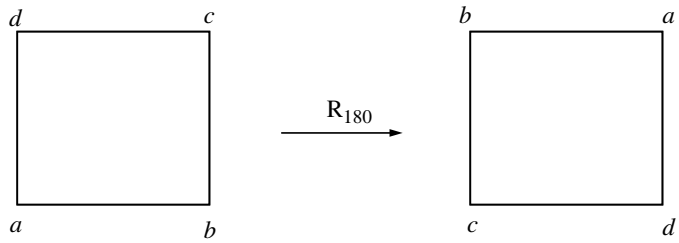
(i) Rotation of 0°:



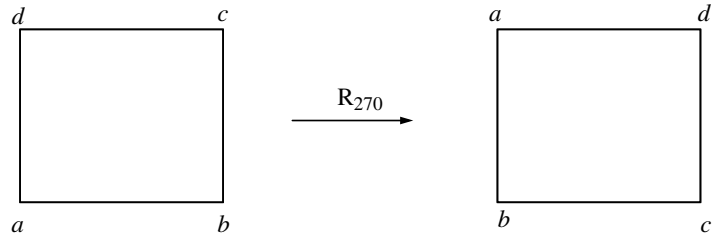
(ii) Rotation of 90°:



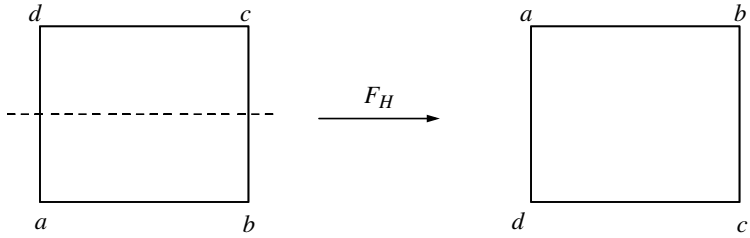
(iii) Rotation of 180°:



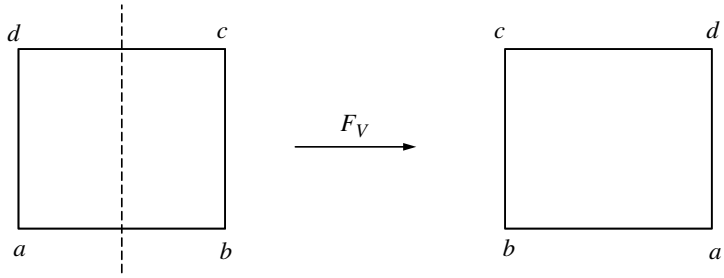
(iv) Rotation of 270°:



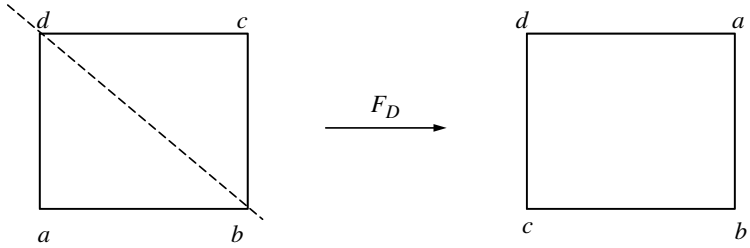
(v) Reflection about the horizontal axis:



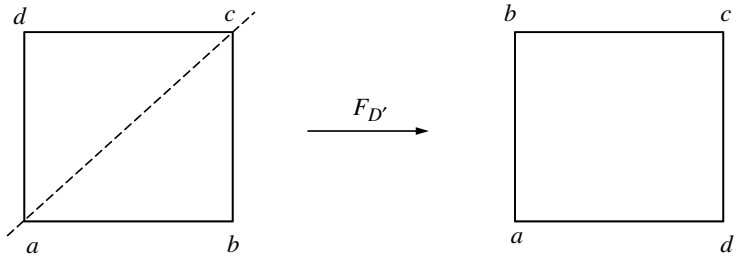
(vi) Reflection about the vertical axis:



(vii) Reflection about the main diagonal:



(viii) Reflection about the other diagonal:



Let $G = \{R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_D, F_{D'}\}$.

Then under the operation of function composition, the Cayley table of G is

Table 1.12: Cayley Table of G

	R_0	R_{90}	R_{180}	R_{270}	F_H	F_V	F_D	$F_{D'}$
R_0	R_0	R_{90}	R_{180}	R_{270}	F_H	F_V	F_D	$F_{D'}$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_{D'}$	F_D	F_H	F_V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_V	F_H	$F_{D'}$	F_D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	F_D	$F_{D'}$	F_V	F_H
F_H	F_H	F_D	F_V	$F_{D'}$	R_0	R_{180}	R_{90}	R_{270}
F_V	F_V	$F_{D'}$	F_H	F_D	R_{180}	R_0	R_{270}	R_{90}
F_D	F_D	F_V	$F_{D'}$	F_H	R_{270}	R_{90}	R_0	R_{180}
$F_{D'}$	$F_{D'}$	F_H	F_D	F_V	R_{90}	R_{270}	R_{180}	R_0

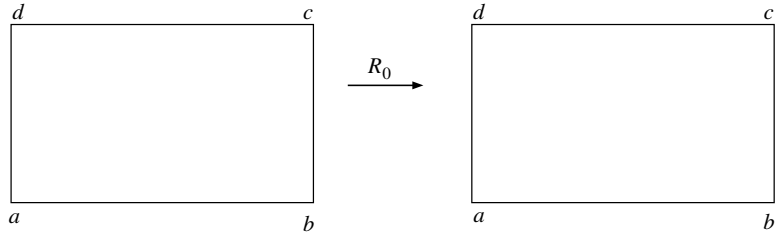
Clearly, from the Cayley table, G forms a group with R_0 acting as the identity element. The inverse of R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_D, $F_{D'}$ are R_0, R_{270}, R_{180}, R_{90}, F_H, F_V, F_D, $F_{D'}$ respectively. Since $F_{D'}F_H \neq F_HF_{D'}$, we have that G is non–abelian.

This group is called a **Dihedral group of order eight** and is denoted by D_4. Hence D_4 is a finite non–abelian group containing eight elements of which four are rotations and four are reflections.

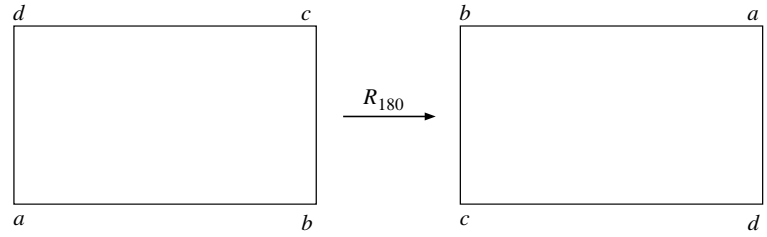
Problem 1.51 Describe the symmetries of a non-square rectangle and construct the corresponding Cayley table. Is the group abelian?

Solution Consider a non-square rectangle and mark its corners as a, b, c and d. The possible rotations and reflections that preserve the original position of the rectangle are

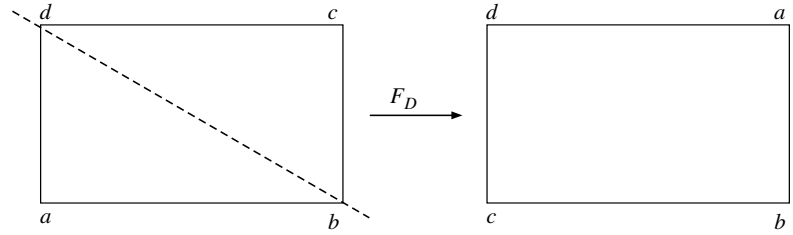
(i) Rotation by 0°:



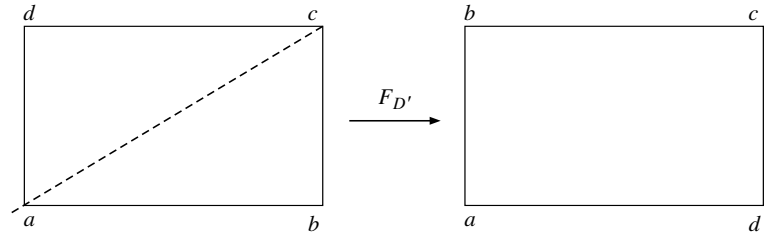
(ii) Rotation by 180°:



(iii) Reflection about the main diagonal:



(iv) Reflection about the other diagonal:



We observe that these are the only possible ways in which we can rotate or reflect the rectangle retaining its position and shape.

Let $G = \{R_0, R_{180}, F_D, F_{D'}\}$. Then under the operation of function composition, the Cayley table of G is

Table 1.14: Cayley Table of G

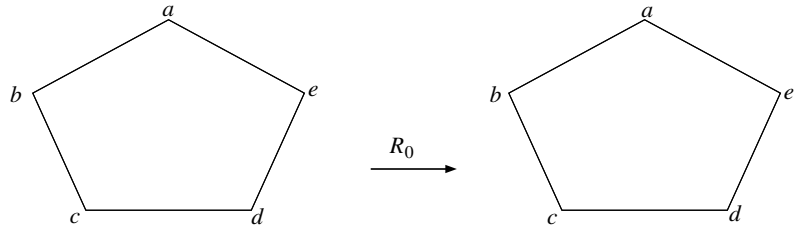
	R_0	R_{180}	F_D	$F_{D'}$
R_0	R_0	R_{180}	F_D	$F_{D'}$
R_{180}	R_{180}	R_0	$F_{D'}$	F_D
F_D	F_D	$F_{D'}$	R_0	R_{180}
$F_{D'}$	$F_{D'}$	F_D	R_{180}	R_0

The set G under function composition satisfies all the group axioms with R_0 being the identity element and every element is inverse of itself. Thus, G forms a group with four elements. From the table we can see that the group is abelian. Therefore G is an example of a finite abelian group whose every element is self-invertible.

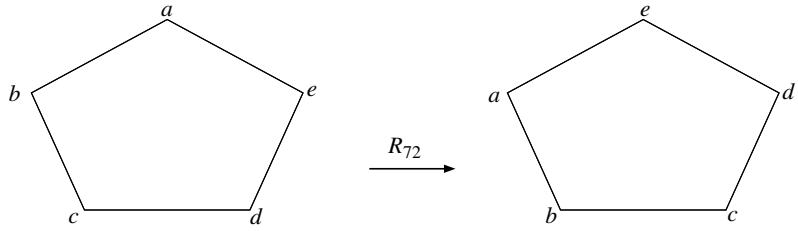
PROBLEM 1.52 Describe the symmetries of a regular pentagon and construct the corresponding Cayley table. Is the group abelian?

SOLUTION Label the vertices of the regular pentagon as a, b, c, d, e. Consider all the possible rotations and reflections that will retain the shape and position of the pentagon.

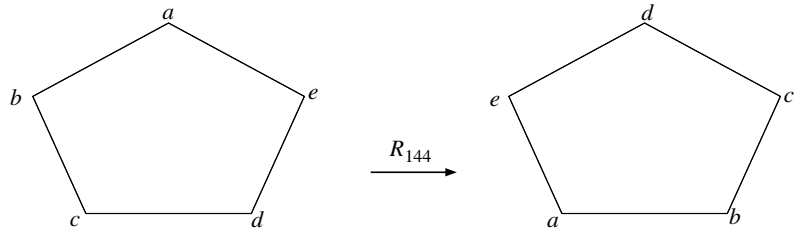
(i) Rotation by 0°:



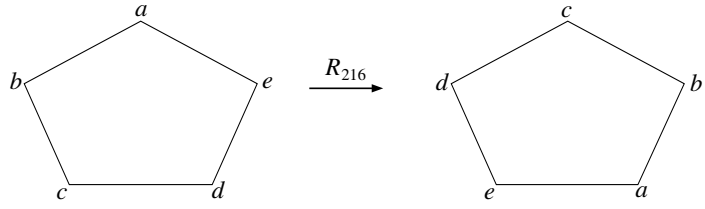
(ii) Rotation by 72°:



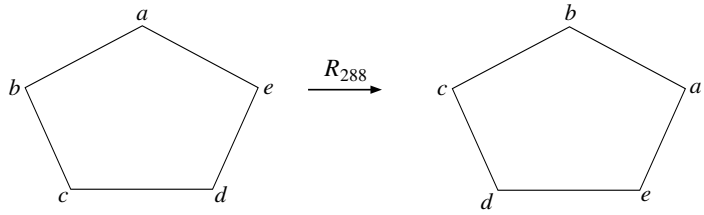
(iii) Rotation by 144°:



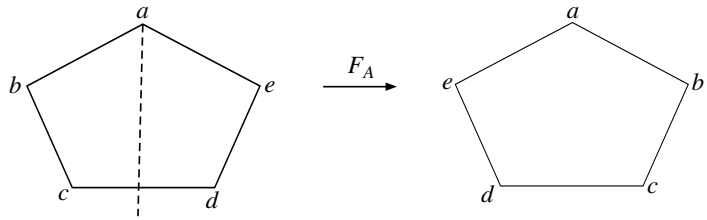
(iv) Rotation by 216°:



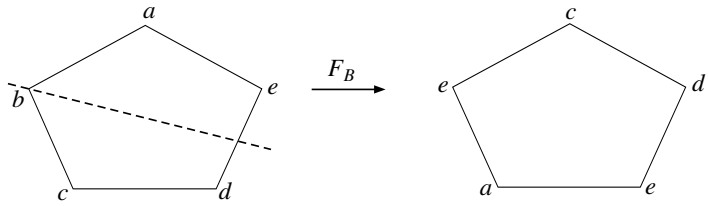
(v) Rotation by 288°:



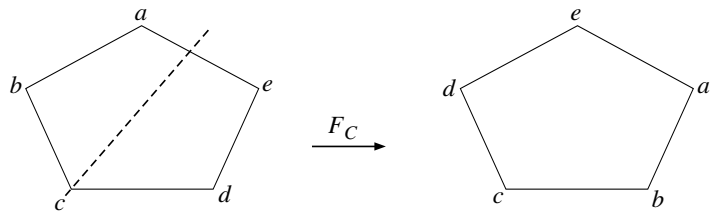
(vi) Reflection about a line passing through a:



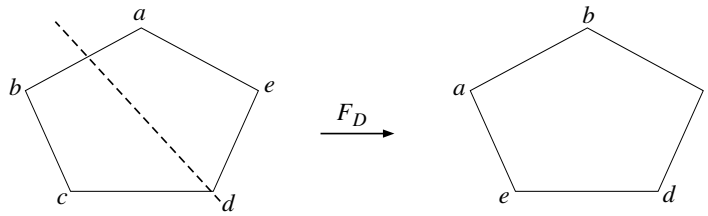
(vii) Reflection about a line passing through b:



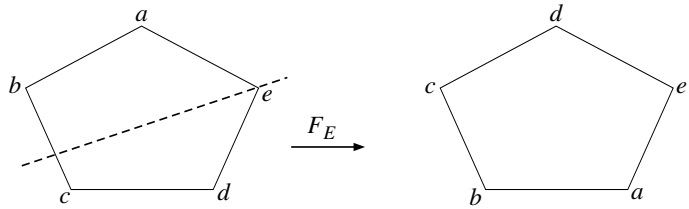
(viii) Reflection about a line passing through c:



(ix) Reflection about a line passing through d:



(x) Reflection about a line passing through e:



Let $G = \{R_0, R_{72}, R_{144}, R_{216}, R_{288}, F_A, F_B, F_C, F_D, F_E\}$. Then under the operation of function composition, the Cayley table of G is

Table 1.15: Cayley Table of G

	R_0	R_{72}	R_{144}	R_{216}	R_{288}	F_A	F_B	F_C	F_D	F_E
R_0	R_0	R_{72}	R_{144}	R_{216}	R_{288}	F_A	F_B	F_C	F_D	F_E
R_{72}	R_{72}	R_{144}	R_{216}	R_{288}	R_0	F_D	F_E	F_A	F_B	F_C
R_{144}	R_{144}	R_{216}	R_{288}	R_0	R_{72}	F_B	F_C	F_D	F_E	F_A
R_{216}	R_{216}	R_{288}	R_0	R_{72}	R_{144}	F_E	F_A	F_B	F_C	F_D
R_{288}	R_{288}	R_0	R_{72}	R_{144}	R_{216}	F_C	F_D	F_E	F_A	F_B
F_A	F_A	F_C	F_E	F_B	F_D	R_0	R_{216}	R_{72}	R_{288}	R_{144}
F_B	F_B	F_D	F_A	F_C	F_E	R_{144}	R_0	R_{216}	R_{72}	R_{288}
F_C	F_C	F_E	F_B	F_D	F_A	R_{288}	R_{144}	R_0	R_{216}	R_{72}
F_D	F_D	F_A	F_C	F_E	F_B	R_{72}	R_{288}	R_{144}	R_0	R_{216}
F_E	F_E	F_B	F_D	F_A	F_C	R_{216}	R_{72}	R_{288}	R_{144}	R_0

From the table it can be seen that closure holds in G. Also function composition is always associative. R_0 acts as the identity element of G. The inverse of R_0, R_{72}, R_{144}, R_{216}, R_{288}, F_A, F_B, F_C, F_D, F_E is R_0, R_{288}, R_{216}, R_{144}, R_{72}, F_A, F_B, F_C, F_D, F_E, respectively.

Thus G forms a group. Also $F_A F_B \neq F_B F_A$.

Therefore, G is a finite non- abelian group of order 10. This group is denoted by D_5.

Remark: In general, for any regular polygon with n sides ($n \geq 3$), the corresponding dihedral group is denoted by D_n and it contains $2n$ elements. Out of these $2n$ elements, n are rotations given by $(2\pi/n)$ and n elements are reflections.

Exercises

1. Give an example of an infinite and a finite group in which each element is its own inverse.

2. Show that the set {5, 15, 25, 35} is a group under multiplication modulo 40.

3. Show that the set $G = \{1, 2, 3, 4, 5\}$ is not a group w.r.t. multiplication modulo 6.

4. Show that the set $G = \{1, 2, 3, 4\}$ is an abelian group w.r.t. multiplication modulo 5.

5. Show that the set $G = \{1, 5, 7, 11\}$ is a group w.r.t. multiplication modulo 12.

6. Show that the set $G = \{2, 4, 8\}$ is a group w.r.t. multiplication modulo 14.

7. Show that the set $G = \{1, 2, 3, 4, 5, 6\}$ is a group w.r.t. multiplication modulo 7.

8. Show that the set $U(15) = \{x \in \mathbb{Z} \mid 1 \leq x < 15, \gcd(x, 15)\}$ is an abelian group under multiplication modulo 15.

9. Prove that the set $G = \left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\right\}$ forms a group under matrix multiplication.

10. Prove that the set $U(7) = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group w.r.t multiplication modulo 7.

11. Give two reasons to show that the set of all odd integers under addition is not a group.

12. Describe the symmetries of a regular hexagon and construct the corresponding Cayley table. Is the group abelian?

13. Find the inverse of $A = \begin{bmatrix}1 & 5\\ 6 & 3\end{bmatrix}$ in $\mathbb{Z}_7$.

14. Construct the Cayley table for $U(12)$.

15. Let $G = \{3^n : n \in \mathbb{Z}\}$. Prove that $(G, .)$ is an abelian group.

16. Prove that every group of order 3 is abelian.

17. Show that a finite semi-group in which cross cancellation holds is an abelian group.

18. Let G be a group and suppose there exist two relatively prime positive integers m and n such that $a^m b^m = b^m a^m$ and $a^n b^n = b^n a^n$ for all $a, b \in G$. Show that G is abelian.

19. In the following, determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.

(a) G = set of all integers, $a \cdot b = a - b$.

(b) $G = a_0, a_1, \ldots, a_6$ where

$$a_i \cdot a_j = a_{i+j}, \text{ if } i + j < 7,$$

$$a_i \cdot a_j = a_{i+j-7}, \text{ if } i + j \geq 7,$$

(c) G = set of all rational numbers with odd denominators, $a \cdot b = a + b$, the usual addition of rational numbers.

20. Show that the set of rational numbers under division does not form a group.

21. Let G be the set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where a, b, c, d are integers modulo 2, such that $ad - bc \neq 0$. Using matrix multiplication as the operation in G, prove that G is a group of order 6.

22. Give an example of a semi-group S which has a right identity and left inverse for each of its elements but it fails to be a group.

Hints to Selected Problems

2. Let $G = \{5, 15, 25, 35\}$

The Cayley Table for G is

$\odot_{40}$	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

Clearly G is closed under $\otimes_{40}$.

Also, associativity holds.

Identity element is 25.

Inverse of 5, 15, 25, 35 is 5, 15, 25, 35 respectively. Therefore, G is a group under $\otimes_{40}$.

19. (a) Since $a - b \in G$, $\forall\ a, b \in G$, so the closure property holds good.

Now, $a \cdot (b \cdot c) = a \cdot (b - c) = a - (b - c) = a - b + c$

On the other hand, $(a \cdot b) \cdot c = (a - b) \cdot c = (a - b) - c = a - b - c$

Since $a \cdot (b \cdot c) \neq (a \cdot b) \cdot c$, therefore associativity does not hold good. Hence, G is not a group.

(b) We can easily check G is a group with a_0 as identity element and a_{7-i} as inverse element of a_i.

(c) Again, we can easily check G is a group with 0 as identity and $-m/n$ as inverse element of m/n.

❑❑❑

2

Finite Groups and Subgroups

Learning Objectives

- Finite Groups
- Definition and Examples of Subgroups
- Subgroup Tests
- Special Class of Subgroups
- Intersection and Union of Subgroups
- Product of two Subgroups

The study of finite groups has been an integral component of group theory since it first emerged in the 19th century. Finite groups often arise while considering symmetrical objects, when those objects admit just a finite number of structure-preserving transformations. Important examples of finite groups include cyclic groups and permutation groups, which we shall study in the next two chapters. The properties of finite groups play a vital role in subjects such as theoretical physics and chemistry.

When one group is completely contained in another, the inner group is called a subgroup of the outer one.

Why do subgroups become important when analyzing groups?

Subgroups are of utmost interest as the study of subgroups of a given finite group can yield a better, more fruitful understanding of that group.

2.1 Finite Groups

We define the order of a group as well as the order of an element of a group and give some examples. We study some useful results based on the definition of order of an element of a group.

© The Author(s) 2023

D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_2

Definition 2.1: The **order of the group** is defined as the number of elements in a group.

Order of G is denoted by $|G|$ or $o(G)$.

For example, the group $\mathbb{Z}$ of integers under addition has infinite order, whereas the group $U(12) = \{1, 5, 7, 11\}$ under multiplication modulo 10 has order 4.

The group $\mathbb{Z}_n$, under addition modulo n, has order n.

Definition 2.2: Let $a \in G$. The **order of an element** a in a group G is the least positive integer n such that $a^n = e$, where $e \in G$ is the identity of the group.

In this case, we write $o(a) = n$.

If no such positive integer exists, then we say that a has infinite order.

The order of an element a is denoted by $|a|$ or $o(a)$.

Remarks:

- To find the order of a group element a, we need to compute the sequence of products $a, a^2, a^3, a^4, \ldots \ldots$ until we reach the identity for the first time. The exponent of this product is the order of a. If the identity never appears in the sequence, then a has infinite order.
- If the group G is defined under addition, then the order of an element $a \in G$ is defined to be the least positive integer n such that $na = 0$.
- To find the order of an element in an additive group, we find the sequence $a, 2a, 3a, \ldots$ until we reach the identity 0 of the group. The coefficient of this product is the order of a.

Example 2.1: Consider $G = \{1, -1, i, -i\}$ under multiplication.

We know that G is a group under multiplication with identity element 1.

Then, since $i^2 = -1$, we have $i^3 = -i$ and $i^4 = i^2 \cdot i^2 = -1 \cdot -1 = 1$, therefore $o(i) = 4$.

In the same way

$$o(1) = 1,\ o(-1) = 2,\ o(-i) = 4.$$

Note that in any group, identity element is of order 1 and it is the only element of order 1.

Example 2.2: Consider the group $(\mathbb{Z}, +)$.

Here, every element except the identity 0 has infinite order, since there exists no positive integer n such that $na = 0$ for all $0 \neq a \in \mathbb{Z}$.

Example 2.3: Let $G = U(12) = \{1, 5, 7, 11\}$.

Then, G is a group under multiplication modulo 12.

To compute $o(7)$, we find the sequence $7^1 = 7$, $7^2 = 49 \equiv 1$, therefore $o(7) = 2$.

In the same way, we see that

$$5^1 = 5,\ 5^2 = 25 \equiv 1, \text{ this gives } o(5) = 2.$$

Similarly, we can find the order of 11.

Also, since 1 is the identity element, so $o(1) = 1$.

Example 2.4: Let $G = \mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\}$ under addition modulo 7.

Since $1.3 = 3$, $2.3 = 6$, $3.3 \equiv 2$, $4.3 \equiv 5$, $5.3 \equiv 1$, $6.3 \equiv 4$, $7.3 \equiv 0$, therefore, $o(3) = 7$.

One can similarly find the order of other elements also.

Remarks:

- $o(a) = n$, if and only if
  - (i) $a^n = e$ and
  - (ii) if $a^k = e$ then $n \leq k$.
- If a has infinite order and $a^\alpha = e$ for some α, then α must be 0.

Problem 2.1 For each of the following groups:
(a) $\mathbb{Z}_{12}$, (b) $U(15)$ and (c) D_4,
find the order of the group and the order of each element in the group.
Also, in each case, describe the relationship between the order of the element of the group and the order of the group?

Solution

(a) We have $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ under addition modulo 12.

Then $o(0) = 1$, $o(1) = o(5) = o(7) = o(11) = 12$.

Also $o(2) = o(10) = 6$.

Similarly, $o(3) = o(9) = 4$, $o(6) = 2$, and $o(4) = o(8) = 3$.

We also know that $o(\mathbb{Z}_{12}) = 12$.

(b) We have $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15.

Then $o(1) = 1$, $o(2) = 4$, $o(4) = 2$, $o(7) = 4$, $o(8) = 4$,

and $o(11) = 2$, $o(13) = 4$, $o(14) = 2$.

Also, $o(U(15)) = 8$.

(c) We have $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_D, F_{D'}\}$.

Then we know that D_4 is a group under function composition.

We have $o(R_0) = 1$, $o(R_{90}) = o(R_{270}) = 2$, $o(R_{180}) = 2$

and $o(F_H) = o(F_V) = o(F_D) = o(F_{D'}) = 2$.

Also, $o(D_4) = 8$.

In each case, we observe that the order of each element of the group divides the order of the group.

Problem 2.2 Let x belong to a group. If $x^2 \neq e$ and $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of x?

Solution If $x^4 = e$, then $e = (x^4)^2 = x^8 = x^6 \cdot x^2 = x^2$ (since $x^6 = e$), which contradicts the hypothesis that $x^2 \neq e$.

Similarly, if $x^5 = e$, then it contradicts the above proof that $x^4 \neq e$.

$\therefore$ $x^4 \neq e$ and $x^5 \neq e$. Hence $o(x) = 3$ or 6.

Some Useful Results: The following results may be useful in finding the order of each and every element of a group by finding the order of only some of the elements of that group.

1. $o(a) = o(a^{-1}), \quad \forall a \in G$

   i.e., in any group, any element and its inverse have the same order.

   Proof: Let $o(a) = n \Rightarrow a^n = e \Rightarrow a^{-n} = e^{-1} = e \Rightarrow (a^{-1})^n = e$

   Now, we show that n is the least positive integer such that $(a^{-1})^n = e$

   Let $(a^{-1})^m = e$ for some $m \in \mathbb{Z}^+$.

   Then, $a^{-m} = e \Rightarrow a^m = e^{-1} = e \Rightarrow a^m = e$

   $\Rightarrow \quad m \geq n \qquad (\because o(a) = n)$

   $\therefore \quad o(a^{-1}) = n = o(a)$

2. $o(x^{-1} ax) = o(a), \quad \forall a \in G$

   Proof: Let $o(a) = n$. This implies $a^n = e$.

   Now, $(x^{-1} ax)^n = x^{-1} a^n x = x^{-1} ex = e.$

   Let $(x^{-1} ax)^m = e$, for some $m \in \mathbb{Z}^+$.

   $\Rightarrow \quad x^{-1}a^m x = e \Rightarrow a^m = xex^{-1} = e \Rightarrow a^m = e$

   But $o(a) = n$, so $m \geq n$

   $\therefore \quad o(x^{-1}ax) = n = o(a)$

3. $o(ab) = o(ba), \quad \forall a, b \in G$

   Proof: We have, $ab = b^{-1} (ba) b$

   $\therefore \quad o(ab) = o(b^{-1}(ba)b) = o(ba) \qquad (\because o(x^{-1} ax) = o(a))$

4. Let $a^m = e$, $m \in \mathbb{Z}^+$. Then, $o(a)$ divides m.

   Proof: Since $a^m = e$, therefore $o(a)$ is finite.

   Let $o(a) = n$. Then, n is the least positive integer such that $a^n = e$.

   We need to show $n \mid m$.

   By division algorithm,

   $$m = nq + r, \quad 0 \leq r < n$$

   Now $e = a^m = a^{nq+r} = a^{nq} a^r = (a^n)^q \cdot a^r = e^q \cdot a^r \qquad (\because a^n = e)$

   $= ea^r = a^r, \quad$ where $0 \leq r < n$

Suppose $r \neq 0$, then $0 < r < n$.

But this contradicts the fact that n is the least positive integer such that $a^n = e$.

$\therefore \qquad r = 0.$

$\therefore \qquad m = nq \quad \Rightarrow \quad n|m, \quad$ i.e., $\quad o(a)|m$

5. $o(a^k) = \dfrac{o(a)}{\gcd(o(a), k)}$.

Proof: Let $o(a) = n$. Then, $\gcd(o(a), k) = \gcd(n, k)$

Let $\gcd(n, k) = d$.

We need to show $o(a^k) = \dfrac{n}{d}$

Now, $(a^k)^{n/d} = (a^n)^{k/d} = e^{k/d} = e$ $(\because o(a) = n, \quad \therefore \quad a^n = e)$

Let $(a^k)^m = e$, for some $m \in \mathbb{Z}^+$. Then $a^{km} = e$.

Therefore, $o(a)|km$ (Using Result (4)

Now, $n|km$ gives $\dfrac{n}{d}|\dfrac{k}{d}m$

Since, $\gcd(n, k) = d$, we have $\gcd\left(\dfrac{n}{d}, \dfrac{k}{d}\right) = 1$.

Therefore, $\dfrac{n}{d}$ divides m $(\because$ if $a|bc$ and $\gcd(a, b) = 1$ then $a|c)$

This gives, $m \geq \dfrac{n}{d}$.

Hence, $o(a^k) = \dfrac{n}{d}$, i.e., $o(a^k) = \dfrac{o(a)}{\gcd(o(a), k)}$.

6. $o(ab) = o(a)o(b)$ if $\gcd(o(a), o(b)) = 1$ and $ab = ba$.

Proof: Let $o(a) = m$ and $o(b) = n$.

To show: $o(ab) = mn$.

Now, $(ab)^{mn} = a^{mn} b^{mn}$ $(\because ab = ba)$

$= (a^m)^n (b^n)^m = e^n e^m = ee = e$

$(\because o(a) = m$ and $o(b) = n)$

Let $(ab)^k = e, \quad k \in \mathbb{Z}^+$

$\Rightarrow \qquad a^k b^k = e$ $(\because ab = ba)$

$\Rightarrow \qquad a^k = b^{-k}$

$\Rightarrow \quad a^{kn} = b^{-kn} = (b^n)^{-k} = e^{-k} = e \qquad (\because o(b) = n \ \therefore \ b^n = e)$

$\Rightarrow \quad o(a) \mid kn \qquad (\text{If } a^m = e \text{ then } o(a) \mid m)$

$\Rightarrow \quad m \mid kn \quad \Rightarrow \quad m \mid k \qquad (\because m \mid kn \text{ and } \gcd(m, n) = 1, \ \therefore \ m \mid k)$

Similarly, $n \mid k$. Therefore $\text{lcm}(m, n) \mid k$.

We also know that

$$\text{lcm}(m, n) \ \gcd(m, n) = mn.$$

Now, since $\gcd(m, n) = 1$, therefore, $mn \mid k$.

Hence, $k \geq mn$.

Thus, $o(ab) = mn = o(a) \ o(b)$.

Remark: The conclusion of part 6 may not hold if any of the conditions $ab = ba$ or $\gcd(o(a), o(b)) = 1$ is dropped.

Example 2.5: In the Quarternion group, we have $ij \neq ji$.

Also, $o(ij) = o(k) = 4$ and $o(i)\,o(j) = 4.4 = 16$.

$\therefore \quad o(ij) \neq o(i) \ o(j)$.

Also, in the group $G = \{1, -1, i, -i\}$, we have

$$o(i) = 4 \text{ and } o(-1) = 2.$$

$\therefore \quad \gcd(o(i), o(-1)) = \gcd(4, 2) = 2 \neq 1$

and $\quad o(-1 \cdot i) = o(-i) = 4 \neq o(-1) \ o(i)$

Problem 2.3 Prove that if a is an element of order n and p is prime to n, then a^p is also of order n.

Solution

Let $\quad o(a^p) = m$.

Now, $\quad o(a) = n \quad \Rightarrow \quad a^n = e \quad \Rightarrow \quad (a^n)^p = e^p = e$

$\Rightarrow \quad (a^p)^n = e \quad \Rightarrow \quad o(a^p) \leq n \quad \Rightarrow \quad m \leq n. \qquad ...(1)$

Since p, n are relatively prime, there exist integers x and y such that

$$px + ny = 1.$$

$\therefore \quad a = a^1 = a^{px+ny} = a^{px} \cdot a^{ny} = a^{px} \cdot (a^n)^y = a^{px} \cdot e^y = a^{px} \cdot e$

$$= a^{px} = (a^p)^x.$$

Now $\quad a^m = [(a^p)^x]^m = (a^p)^{mx} = [(a^p)^m]^x$

$$= e^x \qquad [\because o(a^p) = m \Rightarrow (a^p)^m = e]$$

$$= e$$

$\therefore \quad o(a) \leq m \Rightarrow n \leq m \qquad ...(2)$

From (1) and (2), we get $m = n$.

PROBLEM 2.4 If a group contains elements a and b such that $o(a) = 4$, $o(b) = 2$ and $a^3b = ba$, find $o(ab)$

SOLUTION Given: $o(a) = 4$, $o(b) = 2$ and $a^3b = ba$.

Then $(ab)^2 = abab = a(ba)b$ (Associativity)

$= a(a^3b)b$ ($\because a^3b = ba$)

$= a^4b^2$

$= e$ (As $o(a) = 4$, $o(b) = 2$)

Hence, $o(ab)$ divides 2.

Therefore, $o(ab) = 1$ or 2.

Now, if $o(ab) = 1$, then $ab = e$. This implies $abb^{-1} = eb^{-1}$

$\Rightarrow$ $ae = b^{-1}$

$\Rightarrow$ $a = b^{-1}$

$\Rightarrow$ $o(a) = o(b^{-1}) = o(b)$ giving $4 = 2$, which is not possible.

Therefore, $o(ab) \neq 1$.

Hence, $o(ab) = 2$.

PROBLEM 2.5 (a) For the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from the special linear group SL(2, R), find $o(A)$, $o(B)$ and $o(AB)$.

(b) For the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in the special linear group SL(2, R), find the order of A?

If we view $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ as a member of SL(2, Z_p) (p is a prime), what is the order of A?

SOLUTION (a) We have, $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Then $A^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

$\Rightarrow$ $A^2 \cdot A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$\Rightarrow$ $A^4 = I$; Therefore, $o(A) = 4$

Now, we have $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$

$$\Rightarrow \quad B^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\Rightarrow \quad B^3 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$\therefore \quad o(B) = 3.$

Also, $AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$$\Rightarrow \quad (AB)^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

Continue like this, we get

$$(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

Hence, $o(AB)$ is not finite, whereas $o(A)$ and $o(B)$ are finite.

(b) We have for $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in SL (2, R), $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

Therefore $o(A) = \infty$ in SL(2, R).

However, in SL(2, Z_p), we have

$$A^p = \begin{bmatrix} 1 & p \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Therefore $o(A) = p$ in SL(2, Z_p), p prime.

Problem 2.6 If a group contains an element x such that $o(x) = 6$, find $o(x^2)$, $o(x^3)$, $o(x^4)$, $o(x^5)$.

Further, let y be any other element of the group such that $o(y) = 9$, find $o(y^j)$ for $j = 2, 3, ..., 8$.

Solution We have, $o(x) = 6 \quad \Rightarrow \quad x^6 = e$,

Then, $$o(x^2) = \frac{o(x)}{\gcd(o(x), 2)} = \frac{6}{2} = 3, \quad \therefore \quad o(x^2) = 3$$

$$o(x^3) = \frac{o(x)}{\gcd(o(x), 3)} = \frac{6}{3} = 2, \quad \therefore \quad o(x^3) = 2,$$

$$o(x^4) = \frac{o(x)}{\gcd(o(x), 4)} = \frac{6}{2} = 3, \quad \therefore \quad o(x^4) = 3$$

$$o(x^5) = \frac{o(x)}{\gcd(o(x), 5)} = \frac{6}{1} = 6, \quad \therefore \quad o(x^5) = 6.$$

Also, o(y) = 9 $\Rightarrow$ $y^9 = e$.

$$o(y^2) = \frac{o(y)}{\gcd(o(y), 2)} = \frac{9}{1} = 9, \quad \therefore \quad o(y^2) = 9$$

$$o(y^3) = \frac{o(y)}{\gcd(o(y), 3)} = \frac{9}{3} = 3, \quad \therefore \quad o(y^3) = 3$$

$$o(y^4) = \frac{o(y)}{\gcd(o(y), 4)} = \frac{9}{1} = 9, \quad \therefore \quad o(y^4) = 9$$

$$o(y^5) = \frac{o(y)}{\gcd(o(y), 5)} = \frac{9}{1} = 9, \quad \therefore \quad o(y^5) = 9$$

$$o(y^6) = \frac{o(y)}{\gcd(o(y), 6)} = \frac{9}{3} = 3, \quad \therefore \quad o(y^6) = 3$$

$$o(y^7) = \frac{o(y)}{\gcd(o(y), 7)} = \frac{9}{1} = 9, \quad \therefore \quad o(y^7) = 9$$

$$o(y^8) = \frac{o(y)}{\gcd(o(y), 8)} = \frac{9}{1} = 9, \quad \therefore \quad o(y^8) = 9$$

PROBLEM 2.7 Show that in a group of odd order, the equation $x^2 = a$ has a unique solution for all a in G.

SOLUTION Suppose there exist $x, y \in G$ such that $x^2 = y^2 = a$.

Let $o(G) = 2k + 1$, for some $k \in \mathbb{Z}^+$.

Then, $$x = xe = x \cdot x^{2k+1} = x^{2k+2} = (x^2)^{k+1} = (y^2)^{k+1}$$

$\Rightarrow$ $$x = y^{2k+2} = y \cdot y^{2k+1} = ye = y$$

Therefore, the equation $x^2 = a$ has a unique solution for all a in G.

PROBLEM 2.8 If $o(a) = n$ and k / n, prove that $o(a^{n/k}) = k$.

SOLUTION We know,

$$o(a^{n/k}) = \frac{o(a)}{\gcd\left(o(a), \frac{n}{k}\right)} = \frac{n}{\gcd\left(n, \frac{n}{k}\right)} = \frac{n}{n}k = k$$

$\therefore$ $$o(a^{n/k}) = k.$$

Problem 2.9 If in a group G, $a^5 = e$, $aba^{-1} = b^2$ for $a, b \in G$, then show that $o(b) = 31$.

Solution We have, $b^2 = aba^{-1}$

$\Rightarrow$ $b^4 = (aba^{-1})\,(aba^{-1}) = ab(a^{-1}a)\,ba^{-1}$

$= ab^2a^{-1} = a(aba^{-1})a^{-1}$ $(\because\ b^2 = aba^{-1})$

$\therefore$ $b^4 = a^2ba^{-2}$

$\Rightarrow$ $b^8 = (a^2ba^{-2})(a^2ba^{-2}) = a^2b(a^{-2}a^2)\,ba^{-2}$

$= a^2b^2a^{-2} = a^2(aba^{-1})a^{-2}$

$\therefore$ $b^8 = a^3b\,a^{-3}$

Similarly, $b^{16} = a^4\,ba^{-4}$ and $b^{32} = a^5ba^{-5}$

$\therefore$ $b^{32} = ebe^{-1}$ $(\because\ a^5 = e)$

$\Rightarrow$ $b^{32} = b \Rightarrow b^{31}\,b = eb \Rightarrow b^{31} = e$.

Therefore, 31 is the least positive integer such that $b^{31} = e$.

Hence, $o(b) = 31$.

Problem 2.10 Prove that if a group G is of even order, then it has an element $a \neq e$ satisfying $a^2 = e$.

Solution Let $o(G) = 2n$, where n is a positive integer.

The identity element is its own inverse. We shall prove that there must be at least one more element in G which is its own inverse.

We shall prove it by contradiction.

Suppose G has no element, other than the identity element e, which is its own inverse.

We know that if b is the inverse of c, then c is the inverse of b. So excluding the identity element e, the remaining $2n - 1$ elements of G must be divided into pairs of two such that each pair consists of an element and its inverse. But it is not possible as the odd integer $2n - 1$ is not divisible by 2. Hence our assumption is wrong.

Therefore, there is an element $a \neq e$ in G such that $a = a^{-1}$.

$\Rightarrow$ $aa = a^{-1}a \quad \Rightarrow \quad a^2 = e$.

Problem 2.11 Prove that if a group G has order 4, then it must be abelian.

Solution Let $G = \{e, a, b, c\}$ be a group of order 4.

The identity element e is its own inverse. There must be at least one more element in G which is its own inverse.

Let $a^{-1} = a$.

If $b^{-1} = b$ and $c^{-1} = c$, then definitely G is abelian.

If $b^{-1} = c$ then $c^{-1} = b$ and we have $bc = e = cb$.

Also, $a^{-1} = a \quad \Rightarrow \quad aa = e$.

Note that ab must be either equal to b or c.

Since $ab = b \Rightarrow a = e$, therefore ab must be equal to c. Thus, ac must be equal to b. So we have the following composition table.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Clearly, from the Cayley table, we see that composition in G is commutative.

PROBLEM 2.12 For any positive integer n and any angle θ, show that in the group SL(2, R).

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$$

Use this formula to find the order of

$$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix} \text{ and } \begin{bmatrix} \cos\sqrt{2}^\circ & -\sin\sqrt{2}^\circ \\ \sin\sqrt{2}^\circ & \cos\sqrt{2}^\circ \end{bmatrix}$$

SOLUTION It is easy to prove the first part by induction.

Now, $$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix}^n = \begin{bmatrix} \cos n60^\circ & -\sin n60^\circ \\ \sin n60^\circ & \cos n60^\circ \end{bmatrix}$$

For $n = 6$, we have

$$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix}^6 = \begin{bmatrix} \cos 360^\circ & -\sin 360^\circ \\ \sin 360^\circ & \cos 360^\circ \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$\therefore$ Order of $\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix}$ is 6.

Clearly for no n, we have

$$\begin{bmatrix} \cos\sqrt{2}^\circ & -\sin\sqrt{2}^\circ \\ \sin\sqrt{2}^\circ & \cos\sqrt{2}^\circ \end{bmatrix}^n = I$$

$\therefore$ Order of $\begin{bmatrix} \cos\sqrt{2}^\circ & -\sin\sqrt{2}^\circ \\ \sin\sqrt{2}^\circ & \cos\sqrt{2}^\circ \end{bmatrix}$ is infinite.

2.2 Subgroups

We have seen that the set GL(2, R) = $\{A : A$ is 2×2 matrix over R, $|A| \neq 0\}$ is a group under matrix multiplication. Also, we know that the set SL(2, R) = $\{A : A$ is 2×2 matrix over R, $|A| = 1\}$ is a group under matrix multiplication. Further, SL(2, R) is a subset of GL(2, R). This situation arises so often that we introduce a special term to describe such subsets.

Definition 2.3: A non-empty subset H of a group G is said to be a **subgroup** of G if H itself is a group under the operations of G.

When H is a subgroup of G, we write $H \leq G$.

Definition 2.4: If H is a subgroup of G but not equal to G itself, then H is called a **proper subgroup** of G, written as $H < G$.

Remark: It is important to note that if H is a subgroup of G, the operation of H is same as the operation of G.

For example, $\mathbb{Z}_n$ under addition modulo n is not a subgroup of $\mathbb{Z}$ under addition, since addition modulo n is not the operation of $\mathbb{Z}$.

The notion of subgroup is useful in the sense that it provides us with an easy way of showing that certain sets are groups. Indeed, if G is already known to be a group, and H is a subgroup of G, we may conclude that H is a group without having to check all the axioms in the definition of a group.

Definition 2.5: If G is a group with identity element e, then the subsets $\{e\}$ and G are trivially subgroups of G and we call them the **trivial subgroups** of G.

All other subgroups will be called **non-trivial subgroups** of G.

Note that in trying to verify whether or not a given subset of a group is a subgroup, we are spared checking one of the axioms defining a group, namely the associative law. Since the associative law holds universally in a group G, given any subset A of G and any three elements of A, then the associative law certainly holds for them. So we must check, for a given subset A of G, whether A is closed under the operation of G, whether identity element is in A, and finally, given $a \in A$, whether a^{-1} is also in A.

Problem 2.13 Let $G = \{1, -1, i, -i\}$. Then, G is a group under multiplication. Let $H = \{1, -1\}$ and $K = \{1, -1, i\}$. Show that H is a subgroup of G, whereas K is not a subgroup of G.

Solution

(a) Closure: Clearly H is closed under multiplication.

(b) Identity: $1 \in H$ is the identity.

(c) Inverse: Inverse of 1 is 1 and of -1 is -1.

Therefore H is a group under multiplication and hence a subgroup.

But $K = \{1, -1, i\}$ is not a subgroup of G as $-1 \cdot i = -i \notin K$.

2.3 Subgroup Tests

It may be little cumbersome at times to check whether a given subset H of a group G is a subgroup or not, by having to check all the axioms in the definition of a group. The following two theorems (especially the second one) go a long way in simplifying this exercise.

Theorem 2.1: A non-empty subset H of a group G is a subgroup of G if and only if

(i) $a, b \in H \Rightarrow ab \in H$,

(ii) $a \in H \Rightarrow a^{-1} \in H$.

Proof: Let H be a subgroup of G. Then, H itself is a group.

$\therefore a \in H, b \in H \Rightarrow ab \in H$, by closure property.

Also, $a \in H \Rightarrow a^{-1} \in H$.

$\therefore$ (i) and (ii) hold.

Conversely, let (i) and (ii) hold.

To show: H is a subgroup of G.

By (i), closure property holds in H.

Again, $a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow a(bc) = (ab)c$ ($\because$ G is associative)

Hence, associativity holds in H.

Also, for any $a \in H$, by (ii), $a^{-1} \in H$ and so by (i)

$$aa^{-1} \in H \Rightarrow e \in H.$$

Thus, H has identity.

Inverse of each element of H is in H by (ii).

Hence, H satisfies all the conditions in the definition of a group and thus it forms a group and therefore a subgroup of G.

The above theorem is called **Two Step Subgroup Test.**

Theorem 2.2: A non-empty subset H of a group G is a subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof: Let H be a subgroup of G. Then, H is itself a group.

Let $a, b \in H$. To show that $ab^{-1} \in H$.

Since $b \in H$ and H is a group, therefore $b^{-1} \in H$.

Since $a, b^{-1} \in H$, so by closure $ab^{-1} \in H$

Conversely, let $a, b \in H \Rightarrow ab^{-1} \in H$. …(1)

To show: H is a subgroup of G.

Associativity: As $a(bc) = (ab)c$, $\forall\ a, b, c \in G$ and $H \subseteq G$

$\therefore$ $a(bc) = (ab)c$, $\forall\ a, b, c \in H$.

Existence of identity: Since H is non-empty, let $a \in H$.

So, $a, a \in H \Rightarrow aa^{-1} \in H$ (by (1))

$\Rightarrow$ $e \in H$ ($\because aa^{-1} = e$)

Existence of inverse: Consider $a \in H$.

As, $a, e \in H \Rightarrow ea^{-1} \in H$ (by (1))

$\Rightarrow$ $a^{-1} \in H$ ...(2)

Closure: Let $a, b \in H$. To show: $ab \in H$

As $b \in H \Rightarrow b^{-1} \in H$ (by (2))

As $a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H$ (by (1))

$\Rightarrow$ $ab \in H$, i.e., H is closed.

Therefore, H forms a group and hence a subgroup of G.

The above theorem is called **One Step Subgroup Test.**

While dealing with the finite subset of a group, it is easier to use the following subgroup test. It can make a considerable saving in checking whether a given subset H is a subgroup of G.

Theorem 2.3: A non- empty finite subset H of a group G is a subgroup of G if and only if H is closed under the operation of G, i.e., $ab \in H$, for all $a, b \in H$.

Proof: Let H be a subgroup of G. Then, H is itself a group.

$\therefore$ $ab \in H, \quad \forall\ a, b \in H$ (by closure property)

Conversely, let $a, b \in H \Rightarrow ab \in H$.

To show: H is a subgroup of G.

By two step subgroup test, it is enough to show that

$$a \in H \Rightarrow a^{-1} \in H.$$

Let $a \in H$. If $a = e$, then $a^{-1} = a \in H$.

So, let $a \neq$ e. ...(1)

By closure property, $a, a^2, a^3, a^4, \ldots, \in H$ ...(2)

But as H is finite, so $a^i = a^j$ for some $i \neq j$.

Without loss of generality, let $i > j$, i.e., $i - j > 0$, i.e., $i - j \geq 1$

We assert that $i - j \neq 1$. Let $i - j = 1$.

Then $a^i = a^j \Rightarrow a^{i-j} = e$ ...(3)

$\Rightarrow$ $a = e$ ($\because i - j = 1$), which contradicts (1)

$\therefore$ $i - j > 1 \Rightarrow i - j - 1 > 0 \Rightarrow i - j - 1 \geq 1$

From (3) we have $a^{i-j} = e \Rightarrow (a^{i-j})\, a^{-1} = ea^{-1} \Rightarrow a^{i-j-1} = a^{-1}$,

i.e., $a^{-1} = a^{i-j-1}$, where $i - j - 1 \geq 1$

Since by (2), $a^{i-j-1} \in H$, therefore $a^{-1} \in H$.

Hence, H is a subgroup of G.

The above theorem is called **Finite Subgroup Test.**

Remark: It is not necessary for the group to be finite. Only the subset under consideration needs to be finite.

We now consider some examples of subgroups.

Example 2.6: Let G be an abelian group with identity e.

Let $H = \{x \in G : x^2 = e\}$. Show that H is a subgroup of G.

Solution: As $e^2 = e$, so $e \in H$. Hence H is nonempty.

Let $a, b \in H$. To show that $ab^{-1} \in H$.

As $a \in H$ therefore $a^2 = e$. Similarly, $b \in H$ gives $b^2 = e$ ...(1)

In order to show $ab^{-1} \in H$, we need to show that $(ab^{-1})^2 = e$.

Consider $(ab^{-1})^2 = (ab^{-1})\,(ab^{-1}) = a(b^{-1}\, a)\, b^{-1} = a(ab^{-1})b^{-1}$ (as G is Abelian)

$= (aa)\,(b^{-1}b^{-1})$

$= a^2(b^{-1})^2 = a^2(b^2)^{-1}$ $(\because (b^{-1})^n = (b^n)^{-1})$

$= e(e^{-1}) = e$ (by (1))

Therefore, $ab^{-1} \in H$ and hence H is a subgroup of G.

Example 2.7: Let G be an abelian group under multiplication with identity e. Let $H = \{x^2 : x \in G\}$. Show that H is a subgroup of G.

Solution: Let $a^2, b^2 \in H$. To show: $a^2(b^2)^{-1} \in H$.

Now, $a^2(b^2)^{-1} = a^2(b^{-1})^2$ $(\because (b^{-1})^n = (b^n)^{-1})$

$= (aa)\,(b^{-1}b^{-1}) = a(ab^{-1})b^{-1} = a(b^{-1}a)b^{-1}$ (as G is abelian)

$= (ab^{-1})\,(ab^{-1}) = (ab^{-1})^2 \in H$

Therefore, H is a subgroup of G.

Example 2.8: Let G be a group of non-zero real numbers under multiplication, $H = \{x \in G : x = 1$ or x is irrational$\}$ and $K = \{x \in G : x \geq 1\}$. Show that H and K are not subgroups of G.

Solution: We have, $H = \{x \in G : x = 1$ or x is irrational$\}$

Now, $\sqrt{2} \in H$ but $\sqrt{2}.\sqrt{2} = 2 \notin H$,

$\therefore$ closure property is not satisfied. Hence, H is not a subgroup of G.

Also, $K = \{x \in G : x \geq 1\}$

Now, $2 \in K$ but $2^{-1} = \frac{1}{2} \notin K$, $\therefore$ inverse property is not satisfied.

Hence, K is not a subgroup of G.

Problem 2.14 For each divisor k of n, define $U_k(n) = \{x \in U(n) : x = 1 \bmod k\}$ (i.e., the set of all those $x \in U(n)$ which gives remainder 1, when divided by k)

List the elements of $U_4(20)$, $U_5(20)$, $U_5(30)$ and $U_{10}(30)$.

Prove that $U_k(n)$ is a subgroup of $U(n)$.

Solution We have $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

Therefore, $U_4(20) = \{1, 9, 13, 17\}$ and $U_5(20) = \{1, 11\}$

Also, $U(30) = \{1, 3, 7, 11, 13, 17, 19, 23, 29\}$

$\therefore$ $U_5(30) = \{1, 11\}$ and $U_{10}(30) = \{1, 11\}$.

Now, we will show that $U_k(n)$ is a subgroup of $U(n)$.

Firstly, since $1 \in U_k(n)$ therefore $U_k(n) \neq \phi$

Also, $U_k(n)$ is a finite subset of $U(n)$. (In fact $U(n)$ is itself finite)

$\therefore$ By finite subgroup test, it is enough to show that $U_k(n)$ is closed.

Let $a, b \in U_k(n)$. We need to prove that $ab \in U_k(n)$

Now $a, b \in U_k(n)$ gives $a = 1 (\text{mod } k)$ and $b = 1 (\text{mod } k)$.

This implies that $k | a - 1$ and $k | b - 1$.

Therefore, there exist integers λ, μ such that $a - 1 = \lambda k$ and $b - 1 = \mu k$

i.e. $a = \lambda k + 1$ and $b = \mu k + 1$.

Consider $ab - 1 = (\lambda k + 1)(\mu k + 1) - 1 = (\lambda\mu)k^2 + \lambda k + \mu k + 1 - 1$

$= k(\lambda\mu k + \lambda + \mu)$, i.e., $k | ab - 1$.

This gives that $ab = 1 \text{ (mod) } k$. Hence $ab \in U_k(n)$.

Problem 2.15 If H is a proper subgroup of $\mathbb{Z}$ under addition and H contains 18, 30 and 40, then determine H.

Solution We are given H is a proper subgroup of $\mathbb{Z}$ and $18, 30, 40 \in H$.

Then, $30 \in H, 18 \in H \Rightarrow 30 + (-18) = 12 \in H$

$40 \in H, 30 \in H \Rightarrow 40 + (-30) = 10 \in H$

$12 \in H, 10 \in H \Rightarrow 12 + (-10) = 2 \in H$

$\therefore$ $2n \in H, \quad \forall\, n \in \mathbb{Z}$.

(Using the properties of existence of inverse and closure in a group).

$\therefore$ $H \supseteq E$ (set of all even integers) $= \langle 2 \rangle$

Let, if possible, $(2n + 1) \in H$.

Then, by closure, $(2n + 1) + (-2n) \in H$. $(\because\ 2n \in H)$

$\Rightarrow$ $2n + 1 - 2n \in H \Rightarrow 1 \in H$.

Therefore, $n \cdot 1 \in H,\ \forall\ n \in \mathbb{Z} \Rightarrow n \in H,\ \forall\ n \in \mathbb{Z}$

$\therefore$ $\mathbb{Z} \subseteq H \subseteq \mathbb{Z}$, which is a contradiction as $H < \mathbb{Z}$.

Hence, our assumption is wrong.

$\therefore$ $H = E = \langle 2 \rangle$

Problem 2.16 (a) Let G be an Abelian group with identity e and let n be some integer. Prove that the set of all elements of G that satisfy the equation $x^n = e$ is a subgroup of G.

(b) Give an example of a group G in which the set of all elements of G that satisfy the equation $x^2 = e$ does not form a subgroup of G.

Solution

(a) Let $H = \{x \in G \mid x^n = e\}$.

To show: H is a subgroup of G.

Since $e^n = e$, therefore $e \in H$ and so $H \neq \phi$

Now, let $a, b \in H$. Then $a^n = e$ and $b^n = e$.

So, $(ab)^n = a^n b^n = e \cdot e = e, \quad \therefore \quad ab \in H$ ...(1)

Now $a^n = e \quad \Rightarrow \quad (a^n)^{-1} = e^{-1} \quad \Rightarrow \quad (a^{-1})^n = e$.

$\therefore$ $a^{-1} \in H$. ...(2)

Hence, by two step subgroup test, H is a subgroup of G.

(b) In D_4, consider the set $K = \{R_0, R_{180}, F_H, F_V, F_D, F_{D'}\}$.

Then, each $x \in K$ satisfies the condition that $x^2 = e$.

The set K is not closed as $F_H F_D = R_{90} \notin$ K.

Hence, K is not a subgroup of D_4.

Problem 2.17 Show that a group of order 6 cannot have a subgroup of order 4.

Solution Let G be a group such that $o(G) = 6$.

Let, if possible, H be a subgroup of G such that $o(H) = 4$.

Let $x \in G$ be such that $x \notin H$.

Let $H = \{h_1, h_2, h_3, h_4\}$.

Then, $xH = \{xh : h \in H\}$

$= \{xh_1, xh_2, xh_3, xh_4\}$

Claim: H and xH have no common element.

If $h_i = xh_j$ for some i, j.

$\Rightarrow$ $h_i h_j^{-1} = xh_j h_j^{-1} = xe$

$\Rightarrow$ $x = h_i h_j^{-1} \in H$ ($\because h_i, h_j \in H$ and $H \leq G \therefore h_i h_j^{-1} \in H$)

which is a contradiction. Hence our assumption is wrong.

Therefore, a group of order 6 cannot have a subgroup of order 4.

Problem 2.18 Prove that an abelian group with two elements of order 2 must have a subgroup of order 4.

Solution Let G be an abelian group.

Let $a, b \in G$ such that $o(a) = o(b) = 2$, i.e., $a^2 = b^2 = e$ ...(1)

Consider $H = \{e, a, b, ab\}$. To show: $H \leq G$.

Consider the composition table of H.

Table 2.1: Composition Table of H

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

(Since G is abelian,

$\therefore$ $b(ab) = ab^2 = a$, $(ab)(ab) = a^2b^2 = e$ and $a^2 = e$, $b^2 = e$ (by (1))).

As we can see from the table, closure is clearly satisfied.

Since $e \in H$, so identity element belongs to H.

As $a, b, ab, e \in G$ and G is a group, therefore associativity is satisfied.

Also, inverse of each element is the element itself.

$\therefore$ $H \leq G$.

Problem 2.19 Show that $H = \{(1, b) : b \in \mathbb{R}\}$ is a subgroup of the group $G = \{(a, b) : a \neq 0, b \in \mathbb{R}\}$ under the composition $*$ given by $(a, b) * (c, d) = (ac, bc + d)\ \forall\ (a, b), (c, d) \in G$.

Solution Clearly, H is non empty as $(1, 0) \in H$.

For $(1, b), (1, c) \in H$, we have

$$(1, b) * (1, c) = (1 \cdot 1, b \cdot 1 + c) = (1, b + c) \in H$$

Also, for $(1, b) \in H$, there exists $(1, -b) \in H$ such that

$(1, b) * (1, -b) = (1 \cdot 1, b \cdot 1 - b) = (1, 0)$, identity in G.

$\therefore \qquad (1, b)^{-1} = (1, -b) \in H$

Thus, H is a subgroup of G under the given composition.

Problem 2.20 Give an example of a non-abelian group having an abelian subgroup.

Solution Refer to the previous problem, G is a non-abelian group, but H is an abelian subgroup of G, as $\forall\ (1, b), (1, c) \in H$, we have

$(1, b) * (1, c) = (1, b + c) = (1, c + b) = (1, c) * (1, b)$

Problem 2.21 Show that $HH = H$, where H is a subgroup of G.

Solution We have, $HH = \{h_1h_2 : h_1, h_2 \in H\}$

Let $h \in H$. Then, $h = he \in HH$ $\qquad (\because\ e \in H)$

$\Rightarrow \quad H \subseteq HH$.

Now, let $x \in HH$ so that $x = h_1h_2$, where $h_1, h_2 \in H$.

Since H is a subgroup of G, $h_1h_2 \in H$, i.e., $x \in H$.

So, $\quad HH \subseteq H$.

Therefore, $HH = H$.

Problem 2.22 Show that a non empty finite subset H of a group G is a subgroup of G if and only if $HH = H$.

Solution Let H be a subgroup of group G.

Then, we have already proved in the previous problem $HH = H$.

Conversely, let H be a finite subset of G such that $HH = H$.

Then, $\qquad ab \in H, \forall\ a, b \in H$

Therefore, by finite subgroup test, H is a subgroup of G.

PROBLEM 2.23 Show that $H^{-1} = H$, where H is a subgroup of G. Is the converse true? Justify.

SOLUTION Let $x \in H^{-1} \Rightarrow x = h^{-1}$ for some $h \in H$.

$\Rightarrow x \in H$, as H is a subgroup of G.

So, $H^{-1} \subseteq H$.

Conversely, let $h \in H \Rightarrow h^{-1} \in H$, as H is a subgroup of G.

Now, $h = (h^{-1})^{-1} \in H^{-1}$ and so $H \subseteq H^{-1}$.

Therefore, $H^{-1} = H$.

The converse need not be true, i.e., if $H^{-1} = H$, then H need not be a subgroup of G, as shown in the following example:

EXAMPLE 2.9: Let $G = \{1, -1\}$ under multiplication.

Clearly G is a group.

Let $H = \{-1\}$. Since inverse of -1 is -1, therefore $H^{-1} = \{-1\}$.

But $H^{-1} = \{-1\}$ is not a group under multiplication.

($\because (-1)(-1) = 1 \notin H$, $\therefore$ closure is not true)

$\therefore$ H is not a subgroup of G.

PROBLEM 2.24 Prove that the necessary and sufficient condition for a non empty subset H of a group G to be a subgroup of G is that $HH^{-1} \subseteq H$.

SOLUTION **Necessary Part:** Let H be a subgroup of G.

To show: $HH^{-1} \subseteq H$.

Let $ab^{-1} \in HH^{-1}$ (by definition)

Then, $a \in H, b \in H$.

Since H is a group, therefore $b^{-1} \in H$.

So, by closure, $ab^{-1} \in H$.

Thus, $HH^{-1} \subseteq H$.

Sufficient Part: Let $HH^{-1} \subseteq H$.

To show: H is a subgroup of G.

Let $a, b \in H \Rightarrow ab^{-1} \in HH^{-1}$ (by definition)

Since $HH^{-1} \subseteq H \Rightarrow ab^{-1} \in H$

Therefore, by one step subgroup test, H is a subgroup of G.

PROBLEM 2.25 Prove that the necessary and sufficient condition for a non empty subset H of a group G to be a subgroup of G is that $HH^{-1} = H$.

SOLUTION **Necessary Part:**

Let H be a subgroup of G.

Then, we have by the previous problem, $HH^{-1} \subseteq H$ ...(1)

Let e be the identity element in G, $\therefore \quad e \in H$.

Let $h \in H$, $\therefore \quad h = he = he^{-1} \in HH^{-1}$

$\therefore \qquad H \subseteq HH^{-1}$ ...(2)

Therefore, from (1) and (2), we have $HH^{-1} = H$.

Sufficient Part: Let $HH^{-1} = H$

$\Rightarrow \qquad HH^{-1} \subseteq H$

Therefore, H is a subgroup of G.

PROBLEM 2.26 Show that $H = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \neq 0; a, b \in \mathbb{R} \right\}$ is a subgroup of the multiplicative group G of 2×2 non-singular matrices over $\mathbb{R}$.

SOLUTION Let $P = \begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} \in H$, $Q = \begin{bmatrix} a_2 & b_2 \\ 0 & 1 \end{bmatrix} \in H$; where

$a_1, a_2, b_1, b_2 \in \mathbb{R}$; $a_1 \neq 0$, $a_2 \neq 0$

Now, $Q^{-1} = \begin{bmatrix} a_2^{-1} & -\dfrac{b_2}{a_2} \\ 0 & 1 \end{bmatrix}$ and $PQ^{-1} = \begin{bmatrix} a_1 a_2^{-1} & -\dfrac{a_1 b_2}{a_2} + b_1 \\ 0 & 1 \end{bmatrix} \in H$

Therefore, H is a subgroup of G.

PROBLEM 2.27 If a be a fixed element of a group G and $H = \{x \in G : xa^2 = a^2x\}$, then show that H is a subgroup of G.

SOLUTION Let $x, y \in H$ so that $xa^2 = a^2x$ and $ya^2 = a^2y$.

Then, $(xy)a^2 = x(ya^2) = x(a^2y) = (xa^2)y = (a^2x)y = a^2(xy)$.

Therefore, $(xy)a^2 = a^2(xy) \quad \Rightarrow \quad xy \in H \ \ \forall\ x, y \in H$.

Now let $x \in H$ so that $xa^2 = a^2x$.

Then, $(xa^2)^{-1} = (a^2x)^{-1} \Rightarrow a^{-2}x^{-1} = x^{-1}a^{-2} \Rightarrow x^{-1}a^2 = a^2\, x^{-1}$

$\Rightarrow \quad x^{-1} \in H \quad \forall\ x \in H$.

Therefore, H is a subgroup of G.

Problem 2.28 Let G be the group of all positive real numbers under multiplication and R be the group of all real numbers under addition. Is G a subgroup of R?

Solution No, the reason being the composition in G is different from the composition in R.

Problem 2.29 Let H be a subgroup of a group G and let $S = \{x \in G : xH = Hx\}$. Show that S is a subgroup of G.

Solution Let $x, y \in S$, then $xH = Hx$ and $yH = Hy$.

Now, we have $yH = Hy$

$\Rightarrow$ $y^{-1}(yH) = y^{-1}(Hy)$

$\Rightarrow$ $(y^{-1}y)H = (y^{-1}H)y$

$\Rightarrow$ $eH = (y^{-1}H)y$

$\Rightarrow$ $H = (y^{-1}H)y$

$\Rightarrow$ $Hy^{-1} = (y^{-1}H)yy^{-1}$

$\Rightarrow$ $Hy^{-1} = (y^{-1}H)e$

$\Rightarrow$ $Hy^{-1} = y^{-1}H$

$\Rightarrow$ $x(Hy^{-1}) = x(y^{-1}H)$

$\Rightarrow$ $(xH)y^{-1} = (xy^{-1})H$

$\Rightarrow$ $(Hx)y^{-1} = (xy^{-1})H$ $(\because Hx = xH)$

$\Rightarrow$ $H(xy^{-1}) = (xy^{-1})H$

$\Rightarrow$ $xy^{-1} \in S$

Therefore, S is a subgroup of G.

Problem 2.30 Let G be the additive group of integers. Prove that the set of all multiples of integers by fixed integer m is a subgroup of G.

Solution We have $G = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$.

Let $H = \{... , -3m, -2m, -1m, 0, 1m, 2m, 3m, ...\}$

Let $a, b \in H$. Then, $a = rm$, $b = sm$, where $r, s \in \mathbb{Z}$

Now, we have $a - b = rm + (-s)m$

$= (r - s)m \in H$ $[\because r, s \in \mathbb{Z} \Rightarrow r - s \in \mathbb{Z}]$

Therefore, H is a subgroup of G.

PROBLEM 2.31 Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ under addition. Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G : a + b + c + d = 0 \right\}$. Prove that $H \leq G$. What if 0 is replaced by 1?

SOLUTION Since $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in H, \quad \therefore \quad H \neq \phi.$

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in H.$

Now

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(- \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a' & -b' \\ -c' & -d' \end{bmatrix}$$

$$= \begin{bmatrix} a - a' & b - b' \\ c - c' & d - d' \end{bmatrix} \in H$$

$$[\because a + b + c + d = 0 = a' + b' + c' + d'$$
$$\Rightarrow a - a' + b - b' + c - c' + d - d' = 0]$$

$\therefore$ By one step subgroup test, $H \leq G$.

When 0 is replaced by 1, $H \not\leq G$, since it does not contain identity as $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \notin H.$

PROBLEM 2.32 Let $G = GL(2, \mathbb{R})$. Let $H = \{A \in G : |A| \text{ is a power of } 2\}$. Show that $H \leq G$.

SOLUTION Since $|I| = 1 = 2^0 \Rightarrow I \in H$. Therefore, $H \neq \phi$ ...(1)

Now, let $A \in H$, $B \in H$. Then $|A| = 2^n, |B| = 2^m$

$\therefore \quad |AB| = |A||B| = 2^{n+m}, \qquad \therefore \quad AB \in H.$ ...(2)

$|A^{-1}| = |A|^{-1} = (2^n)^{-1} = 2^{-n}, \qquad \therefore \quad A^{-1} \in H.$ ...(3)

From (1), (2), (3) and two step subgroup test, $H \leq G$.

PROBLEM 2.33 Let H be a subgroup of $\mathbb{R}$ under addition.
Let $K = \{2^a : a \in H\}$. Prove that K is a subgroup of $\mathbb{R}^*$ under multiplication.

Solution Since $0 \in H$ $(\because\ H \le (\mathbb{R}, +))$

$\therefore\ \ 2^0 = 1 \in K$. Hence K is non empty. ...(1)

Now, let $a \in H, \quad b \in H$

$\therefore\ \ -b \in H$ $(\because\ H \le (\mathbb{R}, +))$

$\therefore\ \ a - b \in H$ $(\because\ H \le (\mathbb{R}, +))$

So, $2^a \in K, 2^b \in K \ \Rightarrow\ 2^a\,(2^b)^{-1} = 2^{a-b} \in K$ ...(2)

$\therefore$ By (1), (2) and one step subgroup test, $K \le \mathbb{R}^*$.

Problem 2.34 Let $H = \{a + bi : a, b \in \mathbb{R},\ a^2 + b^2 = 1\}$. Prove or disprove that H is a subgroup of $\mathbb{C}^*$ under multiplication. Describe the elements of H geometrically.

Solution Since $1 + 0i = 1$, so $1 \in H,\ \ \therefore H \neq \phi$ ...(1)

Let $a + bi \in H$ and $c + di \in H$. Then, $a^2 + b^2 = 1$ and $c^2 + d^2 = 1$

$$(a + bi)\,(c + di) = (ac - bd) + (bc + ad)i \in H$$

Now $(ac - bd)^2 + (bc + ad)^2 = a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2$

$$= a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)\,(c^2 + d^2) = 1.1 = 1$$

$\therefore\ \ (a + bi)\,(c + di) \in H$ ...(2)

Also, $$(a + bi)^{-1} = \frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = a - bi \in H$$

$\therefore\ \ (a + bi)^{-1} \in H$ ...(3)

From (1), (2), (3) and two step subgroup test, $H \le \mathbb{C}^*$.

Let $z = a + ib \in H$.

Then, $|z|$ = distance of $P(z)$ from origin = $\sqrt{a^2 + b^2} = 1$.

Thus, H represents all points on the circle of radius 1, centered at the origin.

2.4 Special Class of Subgroups

Definition 2.6: The **center of a group** G is the set of all those elements in G that commute with every element of G. It is denoted by $Z(G)$.

Therefore, $Z(G) = \{a \in G :\ ax = xa\ \ \forall\ x \in G\}$

Clearly, G is a abelian if and only if $Z(G) = G$.

Example 2.10: 1. Consider the group of quaternions Q_8, since $1 \cdot x = x \cdot 1\ \ \forall\ x \in Q_8$ and $(-1) \cdot x = x \cdot (-1)$ for all $x \in Q_8$, thus $Z(Q_8) = \{1, -1\}$.

2. Let $G = D_4$, then since R_0 and R_{180} commute with each element of D_4, so $Z(G) = \{R_0, R_{180}\}$
3. Let $G = K_4$, then $Z(G) = \{a, b, c, e\} = G$.

THEOREM 2.4: The center of a group G is a subgroup of G.

Proof: We have, $Z(G) = \{a \in G : ax = xa \ \forall \ x \in G\}$.

Since $ex = xe, \ \forall \ x \in G, \quad \therefore \quad e \in Z(G)$

Hence, $Z(G)$ is non-empty.

We proceed by the two step subgroup test.

1. Let $a, b \in Z(G)$

   To show that $ab \in Z(G)$, we need to prove $(ab)x = x(ab), \forall x \in G$

   Consider $(ab)x = a(bx)$ (Associativity)

   $= a(xb)$ ($\because b \in Z(G)$)

   $= (ax)b$ (Associativity)

   $= (xa)b$ ($\because a \in Z(G)$)

   $= x(ab)$ (Associativity)

   $\therefore \quad ab \in Z(G)$

2. Let $a \in Z(G)$ be any element

   To show: $a^{-1} \in Z(G)$, i.e., $a^{-1}x = xa^{-1}, \quad \forall x \in G$

   Since $a \in Z(G)$, we have $ax = xa, \quad \forall x \in G$

   $\Rightarrow \quad a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$

   $\Rightarrow \quad (a^{-1}a)xa^{-1} = (a^{-1}x)\ (aa^{-1})$ (Associativity)

   $\Rightarrow \quad exa^{-1} = a^{-1}\ xe$ ($\because aa^{-1} = e = a^{-1}\ a$)

   $\Rightarrow \quad xa^{-1} = a^{-1}\ x$ ($\because e$ is identity)

   $\therefore a^{-1} \in Z(G)$. Thus $Z(G)$ is a subgroup of G.

PROBLEM 2.35 Let G be a group and $a \in Z(G)$. In a Cayley table for G, how does the row headed by a compare with the column headed by a?

SOLUTION Both are same.

PROBLEM 2.36 Must the center of a group be Abelian?

SOLUTION Yes, since the elements in the center of a group commute with all the elements.

Definition 2.7: Let 'a' be a fixed element of a group G. The **centralizer of 'a' in G** is the set of all those elements in G that commute with 'a'.

It is denoted by $C_G(a)$. Therefore, $C_G(a) = \{g \in G : ga = ag\}$

Theorem 2.5: For each 'a' in a group G, the centralizer of 'a' is a subgroup of G.

Proof: Since $ea = a = ae$, therefore $e \in C_G(a)$.

Thus, $C_G(a)$ is non empty.

We now proceed by the one step subgroup test.

Let $x, y \in C_G(a)$. To show: $xy^{-1} \in C_G(a)$, i.e., $(xy^{-1})a = a(xy^{-1})$

Consider, $(xy^{-1})a = x(y^{-1}a)$ (Associativity)

$= x(ay^{-1})$ $(\because y \in C_G(a) \Rightarrow ay = ya \Rightarrow y^{-1}a = ay^{-1})$

$= (xa)y^{-1}$ (Associativity)

$= (ax)y^{-1}$ $(\because x \in C_G(a) \Rightarrow ax = xa)$

$= a(xy^{-1})$ (Associativity)

$\therefore \quad xy^{-1} \in C_G(a)$

Thus, $C_G(a)$ is a subgroup of G.

Problem 2.37 Let G be a group and let $a \in G$. Prove that $C_G(a) = C_G(a^{-1})$.

Solution

$x \in C_G(a) \Leftrightarrow xa = ax \ \forall a \in G$

$\Leftrightarrow \quad x(aa^{-1}) = axa^{-1}$ (Right multiplication by a^{-1})

$\Leftrightarrow \quad xe = axa^{-1}$ $(\because aa^{-1} = e)$

$\Leftrightarrow \quad x = axa^{-1}$ $(\because e$ is identity$)$

$\Leftrightarrow \quad a^{-1}x = (a^{-1}a)xa^{-1}$ (Left multiplication by a^{-1})

$\Leftrightarrow \quad a^{-1}x = exa^{-1}$ $(\because a^{-1}a = e)$

$\Leftrightarrow \quad x \in C_G(a^{-1})$

Therefore, $C_G(a) = C_G(a^{-1})$.

Problem 2.38 Let G be a group. Show that $Z(G) = \bigcap_{a \in G} C_G(a)$.

Solution Let $x \in Z(G)$. Then, $xy = yx, \quad \forall\ y \in G$

In particular, $xa = ax, a \in G$

$\Rightarrow \quad x \in C_G(a)$

This is true for all $a \in G$.

$\Rightarrow \quad x \in \bigcap_{a \in G} C_G(a), \quad \therefore \quad Z(G) \subseteq \bigcap_{a \in G} C_G(a)$ ...(1)

Conversely, let $x \in \bigcap_{a \in G} C_G(a)$. Then $x \in C_G(a) \ \forall a \in G$

$\Rightarrow$ $xa = ax, \forall a \in G$

$\Rightarrow$ $x \in Z(G)$

$\Rightarrow$ $\bigcap_{a \in G} C_G(a) \subseteq Z(G)$ ...(2)

$\therefore$ From (1) and (2), we have $Z(G) = \bigcap_{a \in G} C_G(a)$.

PROBLEM 2.39 Let G be a group and let $a \in G$ such that $o(a) = 5$. Show that $C_G(a) = C_G(a^3)$.

SOLUTION Given: $o(a) = 5$, i.e., $a^5 = e$.

To show: $C_G(a) = C_G(a^3)$.

Let $x \in C_G(a)$ (To show: $x \in C_G(a^3)$)

$\Rightarrow$ $xa = ax$ ...(1) (To show: $xa^3 = a^3x$)

Consider $xa^3 = (xa)a^2 = (ax)a^2$ (by (1))

$= a(xa)a$ (by Associativity)

$= a(ax)a$ (by (1))

$= a^2(xa)$ (by Associativity)

$= a^2(ax)$ (by (1))

$= a^3x$.

$\therefore$ $xa^3 = a^3x$, i.e., $x \in C(a^3)$

Hence, $C_G(a) \subseteq C_G(a^3)$ …(A)

Now, let $y \in C_G(a^3)$ (To show: $y \in C_G(a)$)

$\Rightarrow$ $ya^3 = a^3y$ ...(2) (To show $ya = ay$)

Consider $ya = (ya)e = (ya)\ a^5$ ($\because a^5 = e$)

$= ya^6 = (ya^3)a^3 = (a^3y)a^3$ (by (2))

$= a^3(ya^3)$ (by Associativity)

$= a^6y$ (by (2))

$= ay$ ($\because a^5 = e$)

i.e., $ya = ay$, $\therefore$ $y \in C_G(a)$

$\therefore$ $C_G(a^3) \subseteq C_G(a)$ ...(B)

From (*A*) and (*B*), we have $C_G(a^3) = C_G(a)$. Hence proved.

Definition 2.8: Let G be a group. Let H be a subgroup of G and $x \in G$
Then, $xHx^{-1} = \{xhx^{-1} : h \in H\}$ is called a **conjugate of the subgroup** H.

Theorem 2.6: Let G be a group. Let H be a subgroup of G and $x \in G$. Then, xHx^{-1} is a subgroup of G.

Proof: Since $e = xex^{-1}$ and $xex^{-1} \in xHx^{-1} \quad \therefore \quad e \in xHx^{-1}$

$\therefore$ xHx^{-1} is non-empty.

We proceed by two step subgroup test.

1. Let $a, b \in xHx^{-1}$. Since $a \in xHx^{-1}, \quad \therefore \quad a = xh_1x^{-1}$ for some $h_1 \in H$
   Also, $b \in xHx^{-1}, \quad \therefore \quad b = xh_2 x^{-1}$ for some $h_2 \in H$
   Consider $ab = (xh_1x^{-1})\,(xh_2x^{-1}) = xh_1(x^{-1}x)h_2x^{-1}$ (Associativity)
   $= x(h_1h_2)x^{-1}$ ($\because x^{-1}x = e$)
   $\in xHx^{-1}$ ($\because h_1h_2 \in H$ by closure)
2. Let $a \in xHx^{-1}$. To show: $a^{-1} \in xHx^{-1}$
   Since $a \in xHx^{-1}$, therefore $a = xhx^{-1}$ for some $h \in H$.
   $\Rightarrow \quad a^{-1} = (xhx^{-1})^{-1} = (x^{-1})^{-1}\, h^{-1}\, x^{-1} = xh^{-1}x^{-1} \in xHx^{-1} (\because h^{-1} \in H)$
   $\therefore \quad xHx^{-1} \leq G.$ Hence proved.

Definition 2.9: Let G be a group. Let H be a subgroup of G. Then, **Normalizer of subgroup H** in G is defined as

$$N_G(H) = \{x \in G : xHx^{-1} = H\}$$

Theorem 2.7: For any subgroup H of a group G, $N_G(H)$ is a subgroup of G.

Proof: Since $eHe^{-1} = H, \quad \therefore \quad e \in N_G(H)$

$\therefore$ $N_G(H)$ is non empty.

We proceed by the two step subgroup test.

1. Let $x, y \in N_G(H)$. To show: $xy \in N_G(H)$
   Since $x \in N_G(H), \quad \therefore \quad xHx^{-1} = H$
   Also, $y \in N_G(H), \quad \therefore \quad yHy^{-1} = H$
   Now $(xy)H(xy)^{-1} = xyHy^{-1}\, x^{-1} = xHx^{-1} = H$
   Therefore, $xy \in N_G(H)$
2. Let $x \in N_G(H)$. To show: $x^{-1} \in N_G(H)$
   Since $x \in N_G(H), \quad \therefore \quad xHx^{-1} = H \quad \Rightarrow \quad x^{-1}\, xHx^{-1}\, x = x^{-1}\, Hx$
   $\Rightarrow \quad x^{-1}H(x^{-1})^{-1} = H \quad \Rightarrow \quad x^{-1} \in N_G(H)$
   Thus $N_G(H) \leq G.$

DEFINITION 2.10: Let G be a group. Let H be a subgroup of G. Then, **centralizer of subgroup** H is defined as $C_G(H) = \{x \in G : xh = hx, \forall h \in H\}$, i.e., the set of all those elements of G which commute with every element of H.

THEOREM 2.8: For any subgroup H of a group G, $C_G(H)$ is a subgroup of G.

Proof: Since $ey = y = ye, \quad \forall y \in H$

$\therefore \quad e \in C_G(H)$. Therefore $C_G(H)$ is non empty.

We proceed by the one step subgroup test.

Let $\quad x_1, x_2 \in C_G(H)$.

To show: $x_1x_2^{-1} \in C_G(H)$, i.e. $(x_1x_2^{-1})h = h(x_1x_2^{-1}), \forall h \in H$

Consider, $(x_1x_2^{-1})h = x_1(x_2^{-1}h)$ (Associativity)

$= x_1(hx_2^{-1})$

$(\because x_2 \in C_G(H) \Rightarrow hx_2 = x_2h \Rightarrow hx_2^{-1} = x_2^{-1}h)$

$= (x_1h)x_2^{-1}$ (Associativity)

$= (hx_1)x_2^{-1} \qquad (\because x_1 \in C_G(H) \Rightarrow hx_1 = x_1h)$

$= h(x_1x_2^{-1}), \quad \forall h \in H$ (Associativity)

Therefore, $C_G(H) \leq G$.

PROBLEM 2.40 Let $G = \mathrm{GL}(2, \mathbb{R})$.

(a) Find $C_G\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$ (b) $C_G\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$

(c) Find the centre of G.

SOLUTION (a) Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C_G \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.

Then, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\Rightarrow \quad \begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ a & b \end{bmatrix}.$

$\Rightarrow \quad b = c \quad \text{and} \quad b + d = a$

$\Rightarrow \quad b = c \quad \text{and} \quad c + d = a.$

$\therefore \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c+d & c \\ c & d \end{bmatrix}, cd + d^2 \neq c^2$

$\therefore \quad C_G\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{\begin{bmatrix} c+d & c \\ c & d \end{bmatrix} : cd + d^2 \neq c^2, c, d \in \mathbb{R}\right\}$

(b) Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C_G\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$

$$\Rightarrow \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\Rightarrow \quad \begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$$

$$\Rightarrow \quad b = c, \ \ a = d$$

$$\therefore \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$$

$$\therefore \quad C_G\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} : a^2 \neq b^2, a, b \in R\right\}$$

(c) We have $Z(G) = \{A \in G : AB = BA \text{ for all } B \in G\}$

Let $A = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in Z(G)$ and $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ be any element.

Then $AB = BA$ gives

$$\begin{bmatrix} ax + yc & bx + dy \\ az + cw & bz + dw \end{bmatrix} = \begin{bmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{bmatrix}$$

$$\Rightarrow \quad ax + cy = ax + bz$$

$$bx + dy = ay + bw$$

$$az + cw = cx + dz$$

$$cy + dw = bz + dw$$

Now $ax + cy = ax + bz$ gives $cy = bz$.

Since the matrix B was choosen arbitrarily, the relationship $cy = bz$ must hold for any choice of b and c.

Thus, the only values of y and z for which $cy = bz$ is $y = z = 0$.

Now $bx + dy = ay + bw$ gives $bx = bw \ \Rightarrow \ x = w$

$$\therefore \quad A = \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$$

$$\Rightarrow \quad Z(G) = \left\{\begin{bmatrix} x & \\ 0 & x \end{bmatrix} \middle| \begin{matrix} x \in \mathbb{R} \\ x \neq 0 \end{matrix}\right\}$$

Definition 2.11: Let G be a group and let $a \in G$. Let $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.
Then, $\langle a \rangle$ is called the **cyclic subgroup of the group G generated by a.**

Theorem 2.9: $\langle a \rangle$ is a subgroup of G.

Proof: Since $a \in \langle a \rangle$, $\therefore \langle a \rangle$ is non-empty.

Let $a^n, a^m \in \langle a \rangle$. Then $a^n \cdot a^m = a^{n+m} \in \langle a \rangle$

Let $a^n \in \langle a \rangle$. Then $(a^n)^{-1} = a^{-n} \in \langle a \rangle$.

$\therefore$ $\langle a \rangle$ is a subgroup of G.

Remark: Since $a^n.a^m = a^{n+m} = a^{m+n} = a^m.a^n$, therefore $\langle a \rangle$ is abelian.

Example 2.11: In the group $U(10)$, find the cyclic subgroup generated by 3.

Solution: In $U(10)$, $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$,
as $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv 7$, $3^4 = 81 \equiv 1$, $3^5 = 3^4 \cdot 3 \equiv 3$, $3^6 = 3^4 \cdot 3^2 \equiv 9$, $3^{-1} \equiv 7$, (since $3.7 = 1$), $3^{-2} \equiv 9$ (as $9.9 = 1$), $3^{-3} \equiv 3$, $3^{-4} \equiv 1$, $3^{-5} = 3^{-4} \cdot 3^{-1} \equiv 7$, $3^{-6} = 3^{-4} \cdot 3^{-2} = 9$, ...

Remark: Remember a^n means na, when the operation is addition.

Example 2.12: In the group $\mathbb{Z}_{10}$ find the cyclic subgroup generated by 2.

Solution: In $\mathbb{Z}_{10}$, $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$.

Example 2.13: In $\mathbb{Z}$, $\langle -1 \rangle = \mathbb{Z}$, because each entry in the list ... $(-2)(-1)$, $(-1)(-1)$, $0(-1)$, $1(-1)$, $2(-1)$, ... represents a distinct element of $\mathbb{Z}$.

Example 2.14: In Q_8, $\langle i \rangle = \{1, i, -1, -i\} = \langle -i \rangle$.

Problem 2.41 Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$. Is $U(14) = \langle 11 \rangle$?

Solution

$$\langle 3 \rangle = \{3, 3^2, 3^4, 3^5, 3^6\} = \{3, 9, 13, 11, 15, 1\} = U(14)$$

$$\langle 5 \rangle = \{5, 5^2, 5^3, 5^4, 5^5, 5^6\} = \{5, 11, 13, 9, 3, 1\} = U(14)$$

$$\langle 11 \rangle = \{11, 9, 1\} \neq U(14)$$

$\therefore$ $U(14) = \langle 3 \rangle = \langle 5 \rangle$. But $U(14) \neq \langle 11 \rangle$

Problem 2.42 Find a cyclic subgroup of order 4 in $U(40)$.

Solution

$$U(40) = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$$

$$\langle 3 \rangle = \{3^1, 3^2, 3^3, 3^4\} = \{1, 3, 9, 27\}$$

Clearly, $\langle 3\rangle \leq U(40)$.

Problem 2.43 Find a non-cyclic subgroup of order 4 in $U(40)$.

Solution $\{1, 9, 11, 19\} \leq U(40)$.

Problem 2.44 Show that $\mathbb{Z}_{10} = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle$. Is $\mathbb{Z}_{10} = \langle 2\rangle$?

Solution We know

$$\mathbb{Z}_{10} = \{0, 1, 3, 4, 5, 6, , 7, 8, 9\}, \ \oplus_{10}.$$
$$\langle 3\rangle = \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\} = \mathbb{Z}_{10}$$
$$\langle 7\rangle = \{7, 4, 1, 8, 5, 2, 9, 6, 3, 0\} = \mathbb{Z}_{10}$$
$$\langle 9\rangle = \{9, 8, 7, 6, 5, 4, 3, 2, 1, 0\} = \mathbb{Z}_{10}$$
$$\therefore \quad \mathbb{Z}_{10} = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle.$$

However, $\langle 2\rangle = \{2, 4, 6, 8, 0\} \neq \mathbb{Z}_{10}$.

$$\therefore \quad \langle 2\rangle \neq Z_{10}.$$

Problem 2.45 Show that $U(20) \neq \langle k\rangle$ for any k in $U(20)$.

Solution

$$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\},$$
$$\langle 3\rangle = \{3, 9, 7, 1\}, \ \because \ 3^4 = 1$$
$$\langle 7\rangle = \{7, 9, 3, 1\}, \ \because \ 7^4 = 1.$$
$$\langle 9\rangle = \{9, 1\}, \ \because \ 9^2 = 1$$
$$\langle 11\rangle = \{11, 1\}, \ \because \ 11^2 = 1$$
$$\langle 13\rangle = \{13, 9, 17, 1\}, \ \because \ 13^4 = 1$$
$$\langle 17\rangle = \{17, 9, 13, 1\}, \ \because \ 17^4 = 1$$
$$\langle 19\rangle = \{19, 1\}, \ \because \ 19^2 = 1$$
$$\langle 1\rangle = \{1\}, \ \because \ 1^1 = 1.$$
$$\therefore \quad U(20) \neq \langle k\rangle \text{ for any } k \text{ in } U(20).$$

Problem 2.46 Let $\mathbb{Q}$ be the group of rational numbers under addition and let $\mathbb{Q}^*$ be the group of non-zero rational numbers under multiplication. In $\mathbb{Q}$, list the elements in $\langle 1/2\rangle$. In $\mathbb{Q}^*$, list the elements in $\langle 1/2\rangle$.

Find the order of each element in $\mathbb{Q}$ and in $\mathbb{Q}^*$.

SOLUTION In $\mathbb{Q}$, $\left\langle \frac{1}{2} \right\rangle = \left\{ n\left(\frac{1}{2}\right) : n \in \mathbb{Z} \right\} = \left\{ 0, \pm\frac{1}{2}, \pm 1, \pm\frac{3}{2}, \pm 2, ... \right\}$.

In $\mathbb{Q}^*$, $\left\langle \frac{1}{2} \right\rangle = \left\{ \left(\frac{1}{2}\right)^n : n \in \mathbb{Z} \right\} = \left\{ 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, ..., 2, 4, 8, ... \right\}$

Also, in $\mathbb{Q}$, $o(0) = 1$ and all other elements have infinite order since $x + x + ... + x = 0$ only when $x = 0$.

In $\mathbb{Q}^*$, $o(1) = 1$, $o(-1) = 2$ and all other elements have infinite order since $x \cdot x \cdot x ... x = 1$ only when $x = 1$.

PROBLEM 2.47 Suppose G is a group that has exactly eight elements of order 3. How many subgroups of order 3 does G have?

SOLUTION If $o(a) = 3$, then $\{e, a, a^2\}$ is a subgroup.

Let
$$H = \langle x \rangle = \{x, x^2, e\} \leq G$$
$$K = \langle y \rangle = \{y, y^2, e\} \leq G$$
$$L = \langle z \rangle = \{z, z^2, e\} \leq G$$
$$M = \langle u \rangle = \{u, u^2, e\} \leq G$$

And $o(\langle x \rangle) = o(\langle y \rangle) = o(\langle z \rangle) = o(\langle u \rangle) = 3$.

Now
$$o(x^2) = \frac{o(x)}{\gcd(o(x), 2)} = \frac{3}{\gcd(3, 2)} = \frac{3}{1} = 3$$

$\therefore$
$$o(x^2) = o(y^2) = o(z^2) = o(u^2) = 3.$$

$\therefore$ 8 elements of order 3 produce 4 subgroups of order 3.

To show: There are no other subgroups of order 3.

The only other possibility is to have $H = \{e, a, b\}$, $o(a) = o(b) = 3$.

But then ab is a 4th element of H.

$\therefore$ The group has exactly 4 subgroups of order 3.

2.5 INTERSECTION AND UNION OF SUBGROUPS

THEOREM 2.10: Intersection of a finite class of subgroups is also a subgroup.

Proof: Let $H_1, H_2, ... , H_n$ be subgroups of a group G and let $H = \bigcap_{i=1}^{n} H_i$.

To show that $H \leq G$.

Since $e \in H_1, H_2, \ldots, H_n$ ($\because$ each H_i is a subgroup)

$\therefore$ $e \in \bigcap_{i=1}^{n} H_i$, i.e., $e \in H$.

Therefore, H is non-empty.

Let $a, b \in H$. To show that $ab^{-1} \in H$.

Now, $a, b \in H \Rightarrow a, b \in H_i \; \forall i$

$\Rightarrow$ $ab^{-1} \in H_i \; \forall i$ ($\because H_i \leq G$)

$\Rightarrow$ $ab^{-1} \in \bigcap_{i=1}^{n} H_i$, i.e., $ab^{-1} \in H$

Therefore, H is a subgroup of G.

In particular, if A and B are 2 subgroups of G, then $A \cap B$ is also a subgroup of G.

But the union of two subgroups may not be a subgroup, as shown in the following example:

Example 2.15: Let $G = (\mathbb{Z}, +)$.

Let $A = \langle 2 \rangle = \{0, \pm 2, \pm 4, \pm 6. \ldots\}$ and $B = \langle 3 \rangle = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

Then, $C = A \cup B = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \ldots\}$ is not a subgroup, as $2, 3 \in C$ but $2 + 3 = 5 \notin C$.

Theorem 2.11: If A and B are subgroups of a group G, then $A \cup B$ is a subgroup of G if and only if either $A \subseteq B$ or $B \subseteq A$.

Proof: Let $A \cup B$ be a subgroup of G. To show: $A \subseteq B$ or $B \subseteq A$

Suppose neither $A \subseteq B$ nor $B \subseteq A$

Now, A is not contained in B implies there exist some $x \in A$ such that $x \notin B$

Also, B is not contained in A implies there exist some $y \in B$ such that $y \notin A$

Now, $x \in A \Rightarrow x \in A \cup B$.

Similarly, $y \in B \Rightarrow y \in A \cup B$

Since $A \cup B \leq G$

$\Rightarrow$ $xy^{-1} \in A \cup B$

$\Rightarrow$ $xy^{-1} \in A$ or $xy^{-1} \in B$

If $xy^{-1} \in A$, also $x \in A \Rightarrow x^{-1} \in A$ (As $A \leq G$)

Therefore $x^{-1}(xy^{-1}) \in A$ (by closure property)

$\Rightarrow$ $(x^{-1}x)\, y^{-1} \in A$

$\Rightarrow$ $ey^{-1} \in A$

$\Rightarrow$ $y^{-1} \in A$

$\Rightarrow$ $(y^{-1})^{-1} = y \in A$, a contradiction.

Similarly, if $xy^{-1} \in B$, also $y \in B$

$\Rightarrow$ $(xy^{-1})y \in B$ as $B \leq G$

$\Rightarrow$ $x(y^{-1}y) \in B$

$\Rightarrow$ $xe \in B$, i.e., $x \in B$, which is a contradiction.

$\therefore$ Our assumption is wrong. Hence $A \subseteq B$ or $B \subseteq A$.

Conversely, suppose $A \subseteq B$ or $B \subseteq A$

To show that $A \cup B \leq G$

If $A \subseteq B \Rightarrow A \cup B = B \Rightarrow A \cup B \leq G$

If $B \subseteq A \Rightarrow A \cup B = A \Rightarrow A \cup B \leq G$

So in either case $A \cup B \leq G$.

2.6 Product of Two Subgroups

We now define the product of two subgroups and study the conditions under which it itself becomes a subgroup.

Definition 2.11: Let H and K be two subgroups of a group G. We define the **product of two subgroups** H and K as

$$HK = \{hk \mid h \in H, k \in K\}$$

and $$KH = \{kh \mid k \in K, h \in H\}$$

Lemma 2.1: Let H and K be two subgroups of a group G.

Then, $x \in HK \Leftrightarrow x^{-1} \in KH$.

Proof: Let $x \in HK \Rightarrow x = hk$ for some $h \in H$, $k \in K$

$\Rightarrow$ $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$

($\because$ $k \in K$ and $K \leq G$, so $k^{-1} \in K$. Similarly, $h^{-1} \in H$ as $H \leq G$)

Conversely, let $x^{-1} \in KH$

$\Rightarrow$ $x^{-1} = kh$ for some $k \in K$ and $h \in H$

$\Rightarrow$ $x = (x^{-1})^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$.

(since $h^{-1} \in H$ and $k^{-1} \in K$ as $H, K \leq G$)

THEOREM 2.12: Let H and K be subgroups of a group G. Then, HK is a subgroup of G if and only if $HK = KH$.

Proof: Let $HK \leq G$. To show: $HK = KH$.

Let $x \in HK \Rightarrow x^{-1} \in HK$ ($\because HK \leq G$)

Then, by lemma, $x \in KH$. Therefore, $HK \subseteq KH$ ...(1)

Now, let $x \in KH \Rightarrow x^{-1} \in HK$ (by Lemma)

$\Rightarrow (x^{-1})^{-1} \in HK$ ($\because HK \leq G$)

$\Rightarrow x \in HK$. Therefore, $KH \subseteq HK$ ...(2)

By (1) and (2), we get $HK = KH$.

Conversely, let $HK = KH$. To show: $HK \leq G$.

Clearly, $HK \neq \phi$ ($\because e \in H, e \in K$ as $H, K \leq G$, $\therefore ee \in HK \Rightarrow e \in HK$)

(i) Let $x, y \in HK$. To show: $xy \in HK$

Since $x, y \in HK \Rightarrow x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Consider, $xy = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$ (By Associative law)

Now, $k_1h_2 \in KH = HK$, $\therefore k_1h_2 = h_3k_3$ for some $h_3 \in H$, $k_3 \in K$

$\therefore xy = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK$ ($\because H \leq G, K \leq G$)

(ii) Let $x \in HK$. To show: $x^{-1} \in HK$

Since $x \in HK \Rightarrow x^{-1} \in KH$ (by Lemma)

$\Rightarrow x^{-1} \in HK$ [$\because HK = KH$]

Hence, $HK \leq G$.

COROLLARY 2.1: Let H and K be 2 subgroups of an abelian group G, then $HK \leq G$.

Proof: Since G is abelian, $HK = KH$. Therefore, $HK \leq G$.
(by converse of previous theorem)

EXERCISES

1. Find the order of each element of Q_8 and D_3.
2. $U(15)$ has six cyclic subgroups. List them.
3. Let $G = GL(2, R)$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a \text{ and } b \text{ are non zero integers} \right\}$.

Prove or disprove that H is a subgroup of G.

4. Let $H = \{a + bi \mid a, b \in R, ab \geq 0\}$ Prove or disprove that H is a subgroup of $\mathbb{C}$ under addition.

5. Find centre of S_3.

6. Let a and b be elements in a finite group G. Prove that $o(ab) = o(ba)$.

7. Prove that if a is the only element of order 2 in a group G, then $a \in Z(G)$.

8. Let a be a non-identity element in a group G such that $O(a) = p$ is a prime number. Prove that $o(a^i) = p$, for each $1 \leq i < p$.

9. Let G be a finite group. Prove that number of elements x of G such that $x^7 = e$ is odd.

10. Let a be an element in a group G such that $a^n = e$ for some positive integer n. If m is a positive integer such that $\gcd(n, m) = 1$, then prove that $a = b^m$ for some b in G.

11. Let a and b be elements in a group such that $ab = ba$ and $o(a) = n$ and $o(b) = m$ and $\gcd(n, m) = 1$. Prove that $o(ab) = \text{lcm}(n, m) = nm$.

12. Let x and y be elements in a group G such that $xy \in Z(G)$. Prove that $xy = yx$.

13. Let D be the set of all elements of finite order in an abelian group G. Prove that D is a subgroup of G.

14. Let G be an abelian group, and let $H = \{a \in G : o(a) = 1 \text{ or } o(a) = 13\}$. Prove that H is a subgroup of G.

15. Let a be an element in a group such that a has infinite order. Prove that $o(a^m)$ is infinite for each $m \in Z$.

16. Find the smallest subgroup of $\mathbb{Z}$ containing

(a) 8, 13 (b) m, n

(c) 6, 15 (d) 8, 14

HINTS TO SELECTED PROBLEMS

2. $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{2, 4, 8, 1\} = \langle 8 \rangle$

$\langle 4 \rangle = \{4, 1\}$

$\langle 7 \rangle = \{7, 4, 13, 1\} = \langle 13 \rangle$

$\langle 11 \rangle = \{11, 1\}$

$\langle 14 \rangle = \{14, 1\}$.

3. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in H$.

Then $A^{-1} = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1/2 \end{bmatrix} \notin H \qquad \left(\because \frac{1}{2} \notin \mathbb{Z}^*\right)$

$\therefore \quad H \not\leq G$.

4. Let $-1 \in H$ and $i \in H$.

Then $-1 + i \notin H \qquad (\because (-1)(1) = -1 < 0)$

$\therefore \quad H \not\leq \mathbb{C}$.

5. $Z(S_3)$ contains only I.

6. Let $n = o(ab)$ and $m = o(ba)$.

Now $(ba)^n = (a^{-1}(ab)a)^n = a^{-1}(ab)^n a = e$. Thus $m|n$.

Also $(ab)^m = (b^{-1}(ba)b)^m = b^{-1}(ba)^m b = e$. Thus $n|m$.

Therefore we have, $n = m$.

7. Let $a \notin Z(G)$. Then, $xa \neq ax$ for some $x \in G$.

So, we have $o(x^{-1}ax) = o(a) = 2$, a contradiction, since a is the only element of order 2 in G. Therefore, $a \in Z(G)$.

8. For each $1 \leq i < p$, we have $(a^i)^p = (a^p)^i = e^i = e$.

Now let $(a^i)^m = e$. To show: $m \geq p$.

We have $(a^i)^m = e \Rightarrow a^{im} = e \Rightarrow p$ divides im as $o(a) = p$

$\Rightarrow$ p divides i or p divides m.

But p cannot divide i as $1 \leq i < p$. Therefore p divides $m \Rightarrow p \leq m$.

10. Since $\gcd(n, m) = 1$, $cn + dm = 1$ for some integers c and d. Hence,

$a = a^1 = a^{cn+dm} = a^{cn} \cdot a^{dm}$. Since $a^n = e$, $a^{cn} = e$.

Hence $a = a^{dm}$. Thus, let $b = a^d$. Hence, $a = b^m$.

12. Since $xy \in Z(G)$, we have $xy = x^{-1}x(xy) = x^{-1}(xy)x = (x^{-1}x)yx = yx$.

13. Let a and b be elements in D, and let $n = o(a)$ and $m = o(b)$. Then

$o(a^{-1}) = n$. Since G is abelian, $(a^{-1}\ b)^{nm} = (a^{-1})^{nm}\ b^{nm} = e$.

Thus $o(a^{-1}b)$ is a finite number as $o(a^{-1}b) \leq nm$.

Hence $a^{-1}b \in D$. Thus, D is a subgroup of G.

14. Let $a, b \in H$. If $a = e$ or $b = e$, then it is clear that $a^{-1} b \in H$.

Hence assume that neither $a = e$ nor $b = e$. Hence, $o(a) = o(b) = 13$.

Thus $o(a^{-1}) = 13$. Hence, $(a^{-1}b)^{13} = (a^{-1})^{13}(b)^{13} = e$.

Thus $o(a^{-1}b)$ divides 13. Since 13 is prime, 1 and 13 are the only divisors of 13. Thus, $o(a^{-1}b)$ is either 1 or 13. Thus, $a^{-1}b \in H$.

Thus H is a subgroup of G.

15. Let $o(a^m)$ be finite, say, n. Then, $(a^m)^n = a^{mn} = e$.

Thus $o(a)$ divides mn. Hence, $o(a)$ is finite, a contradiction.

Therefore $o(a^m)$ is infinite.

❑❑❑

3

Cyclic Groups

Learning Objectives

- Definition of a Cyclic Group and its Properties
- Finding the Number of Elements of a given Order in a Cyclic Group
- Number of Generators of a Cyclic Group
- Classification of Subgroups of Cyclic Groups

In chapter one we established that the dihedral groups describe objects that have both rotational and bilateral symmetry, i.e., they look the same when flipped over in a specific direction, such as horizontally. The most basic family of groups, the cyclic groups, describe objects that have only rotational symmetry. Cyclic groups can be thought of as rotations, rotating an object a certain number of times till we eventually return to the original position. Cyclic groups have applications across a broad spectrum: in the fields of number theory, chaos theory, and cryptography, among others.

3.1 Cyclic Groups and their Properties

We define a cyclic group and generator of a cyclic group and study how to find number of elements of a given order in a cyclic group. We also study various properties of cyclic groups.

Definition 3.1: A group G is called a **cyclic group** if there is an element $a \in G$ such that every element of G is some integral power of a.

The group G is said to be **generated by** $\boldsymbol{a}$ and a is called a **generator of** $\boldsymbol{G}$.

If G is a cyclic group generated by a, we write $G = \{a^n : n \in Z\}$ and denote it by $G = \langle a \rangle$.

© The Author(s) 2023
D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_3

If G is a finite cyclic group of order n, generated by a, then

$$G = \{a, a^2, a^3, \ldots, a^n = e\}$$

Remark: If the binary operation is addition, then $G = \langle a \rangle = \{na : n \in Z\}$

ILLUSTRATIONS:

1. Let $G = (\mathbb{Z}, +)$. Then G is cyclic and $G = \langle 1 \rangle = \langle -1 \rangle$, i.e., 1 and -1 are generators of G.

   It must be noted that when the operation is addition, $1^n = \underbrace{1+1+\ldots+1}_{n \text{ times}}$.

2. Let $G = (m\mathbb{Z}, +)$. Then $G = \langle m \rangle = \langle -m \rangle$
3. The set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ for $n \geq 1$, under addition modulo n, is a finite cyclic group of order n and $\mathbb{Z}_n = \langle 1 \rangle$.

   Remark: Unlike $\mathbb{Z}$, which has only two generators, $\mathbb{Z}_n$ may have many generators depending on n.

   For example: Consider $\mathbb{Z}_8 = \{0, 1, 2, \ldots, 7\}$. We know $\mathbb{Z}_8$ forms a group under $\oplus_8$.

   Also, $\langle 3 \rangle = \{3, (3+3) \bmod 8, (3+3+3) \bmod 8, \ldots\} \equiv \{3, 6, 1, 4, 7, 2, 5, 0\} = \mathbb{Z}_8$.

   Thus, 3 is a generator of $\mathbb{Z}_8$. Also, $\mathbb{Z}_8 = \langle 5 \rangle = \langle 7 \rangle$.

   On the other hand, 4 is not a generator, since $\langle 4 \rangle = \{0, 4\} \neq \mathbb{Z}_8$.

   Similarly, it can be seen that $\langle 2 \rangle = \{0, 2, 4, 6\} \neq \mathbb{Z}_8$.
4. Consider $U(8) = \{1, 3, 5, 7\}$ under multiplication modulo 8.

   Since, $\langle 3 \rangle \neq U(8)$, therefore 3 is not a generator of $U(8)$.

   Similarly, it can be seen that no other element of $U(8)$ acts as a generator of $U(8)$. Hence, $U(8)$ is not cyclic.
5. The group G of n n^{th} roots of unity is a cyclic group.

   We have $G = \{1, e^{2\pi i/n}, e^{4\pi i/n}, e^{6\pi i/n}, \ldots, e^{2(n-1)\pi i/n}\}$

   Let $\omega = e^{2\pi i/n}$

   Then, $\omega^n = 1$ and $G = \{\omega, \omega^2, \omega^3, \ldots, \omega^{n-1}, \omega^n = 1\} = \langle \omega \rangle$.

PROBLEM 3.1 Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$ and is hence cyclic.

SOLUTION We have $U(14) = \{1, 3, 5, 9, 11, 13\}$.

Then $\langle 3 \rangle = \{1, 9, 13, 11, 3, 5\} = \langle 5 \rangle = U(14)$

Also $\langle 11 \rangle = \{11, 9, 1\} \neq U(14)$

Problem 3.2 Show that $U(20)$ is not cyclic.

Solution We have $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

Then

$$\langle 1\rangle = \{1\}$$
$$\langle 3\rangle = \{1, 3, 7, 9\}$$
$$\langle 7\rangle = \{1, 7, 9, 3\}$$
$$\langle 9\rangle = \{1, 9\}$$
$$\langle 11\rangle = \{1, 11\}$$
$$\langle 13\rangle = \{1, 13, 17, 9\}$$
$$\langle 17\rangle = \{17, 9, 13, 1\}$$
$$\langle 19\rangle = \{19, 1\}$$

We observe that there does not exist any $k \in U(20)$ such that

$$U(20) = \langle k\rangle.$$

Hence $U(20)$ is not cyclic.

Theorem 3.1: Every cyclic group is abelian.

Proof: Let G be a cyclic group generated by a, i.e., $G = \langle a\rangle$.

Let $x, y \in G$. Then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbb{Z}$.

Therefore $$xy = a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = yx.$$

Thus G is abelian.

Note: The converse need not be true, i.e., every abelian group may not be cyclic.

For example:

1. Let $G = (Q, +)$. Then, G is abelian.

   Let us assume that G is cyclic. Suppose $G = \left\langle \frac{m}{n} \right\rangle$.

   Since $\frac{1}{2n} \in \mathbb{Q}$, we have $\frac{1}{2n} = r\frac{m}{n}$, for some $r \in \mathbb{Z}$.

   This gives $1 = 2rm$, which is not possible as $r, m \in \mathbb{Z}$.
   Thus G is not cyclic.
2. $G = (U_8, \otimes_8)$ is abelian but not cyclic.
3. The group $K_4 = \{e, a, b, c : a^2 = b^2 = c^2 = e, ab = ba = c\}$ is abelian but not cyclic.

Remark: Clearly, from the above theorem, every non-abelian group is non-cyclic. For example, D_3 is not abelian and hence not cyclic.

3.2 Generators of a Cyclic Group

In the following theorem, we learn how to find the generators of an infinite cyclic group and a finite cyclic group.

Theorem 3.2: Let G be a group and let 'a' $\in G$.

(i) If 'a' has infinite order, then all distinct powers of 'a' are distinct group elements.

(ii) If 'a' has finite order, say n, then $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if $n|i-j$.

Proof:

(i) If 'a' has infinite order, then there is no non-zero n such that $a^n = e$.

To show that all distinct powers of 'a' are distinct group elements.

Let, if possible, $a^i = a^j$ for some $i \neq j$.

$\Rightarrow \quad a^{i-j} = e$

$\Rightarrow \quad i - j = 0$ (as 'a' has infinite order)

$\Rightarrow \quad i = j$, a contradiction.

$\therefore$ All distinct powers of 'a' are distinct group elements.

(ii) Let $o(a) = n$

To show: $o(\langle a\rangle) = n$, i.e., $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

We first show that $e, a, a^2, \ldots, a^{n-1}$ are all distinct elements.

Let $a^i = a^j$, $i, j \in \{0, 1, \ldots, n-1\}$, $i \neq j$.

Let $i > j$, then $i - j \in \{0, 1, \ldots, n-1\}$

Since $a^i = a^j$ we have $a^{i-j} = e$, a contradiction as $i - j < n$ and $o(a) = n$.

Therefore, $a^i \neq a^j \quad \forall i \neq j$ ...(1)

We now show that these are the only elements of $\langle a\rangle$.

Consider $a^k \in \langle a\rangle$. To show: $a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$.

Applying division algorithm to k, n, there exist integers q, r such that $k = nq + r$, $0 \leq r < n$.

Consider $a^k = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e.a^r = a^r$.

$\therefore \quad a^k = a^r$, $0 \leq r < n$, i.e., $a^k = e$ or a or $a^2, \ldots,$ or a^{n-1},

i.e., $a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$ ...(2)

From (1) and (2), we get $e, a, a^2, \ldots, a^{n-1}$ are n distinct elements of $\langle a\rangle$ and any element a^k is of the form $e, a, a^2, \ldots, a^{n-1}$.

We now show that $a^i = a^j$ if and only if $n|(i-j)$.

We now show that these are the only elements of $\langle a \rangle$.

Let $a^i = a^j$, then $a^{i-j} = e$.

Again, applying division algorithm, there exist $q, r \in \mathbb{Z}$ such that

$$i - j = qn + r, \quad 0 \leq r < n.$$

$$\Rightarrow \quad a^{i-j} = a^{qn+r}$$

$$\Rightarrow \quad e = a^{qn} \cdot a^r$$

$$\Rightarrow \quad e = (a^n)^q \cdot a^r$$

$$\Rightarrow \quad e = e \cdot a^r$$

$$\Rightarrow \quad e = a^r, \ 0 \leq r < n$$

Since n is the least positive integer such that $a^n = e$, we must have $r = 0$.

$$\therefore \quad i - j = qn, \quad \text{giving } n|(i - j).$$

Conversely, let $n|(i - j)$, then $(i - j) = nq$, where $q \in \mathbb{Z}$.

Therefore $a^{i-j} = (a^n)^q = e^q = e$. Hence $a^i = a^j$.

Corollary 3.1: Let G be a group. Let $a \in G$ be such that $o(a) = n$. If $a^k = e$, then $n|k$.

Proof: Since $a^k = e$, and also $a^0 = e$, we have $a^k = a^0$.

Therefore, by above theorem, we have $n|k - 0$, i.e., $n|k$.

Theorem 3.3: The order of a cyclic group is equal to the order of its generator.

Proof: Let G be a cyclic group generated by a.

(i) If $o(a)$ is finite, say n, then $G = \{e, a, a^2, a^3, \ldots, a^{n-1}\}$ and so
$$o(G) = o(\langle a \rangle) = n = o(a).$$

(ii) If $o(a)$ is infinite, then all distinct powers of a are distinct group elements. In other words, G would contain infinite number of elements.

Lemma 3.1: If $a \in \langle a^k \rangle$ then $\langle a \rangle \subseteq \langle a^k \rangle$.

Proof: Let $x \in \langle a \rangle$, then $x = a^m$ for some $m \in \mathbb{Z}$.

Since $a \in \langle a^k \rangle$, therefore $a = a^{kp}$, $p \in \mathbb{Z}$.

Then, $x = (a^{kp})^m = (a^k)^{pm} \in \langle a^k \rangle$. Thus $\langle a \rangle \subseteq \langle a^k \rangle$.

Theorem 3.4: Let $G = \langle a \rangle$ be a cyclic group of order n. Then, $G = \langle a^k \rangle$ if and only if gcd $(k, n) = 1$.

Proof: Let $G = \langle a \rangle$ be a cyclic group of order n.

Then $$o(G) = o(\langle a \rangle) = o(a) = n$$

As $o(a) = n$, therefore $a^n = e$. ...(1)

Now first let $G = \langle a^k \rangle$. Then $o(\langle a^k \rangle) = o(a^k) = o(G) = n$ ...(2)

We need to show that gcd(k, n) = 1.

Let, if possible, gcd(k, n) = $d > 1$. Then $d|k$ and $d|n$.

$\Rightarrow$ $k = td$ and $n = sd$, for some $s, t \in \mathbb{Z}$ (Note that $s < n$).

Now consider $(a^k)^s = (a^{td})^s = (a^{sd})^t = (a^n)^t = e^t = e$ (by (1))

$\therefore$ $(a^k)^s = e$, a contradiction as $o(a^k) = n$ and $s < n$.

$\therefore$ gcd (k, n) = 1.

Conversely, let gcd (k, n) = 1. To show: $G = \langle a^k \rangle$.

Since gcd(k, n) = 1, there exist $u, v \in \mathbb{Z}$ such that $1 = ku + nv$.

Consider $a = a^1 = a^{ku+nv} = a^{ku}(a^n)^v = a^{ku} \cdot e^v = a^{ku}$ (by (1))

Therefore, by Lemma, as $a \in \langle a^k \rangle$ we have $\langle a \rangle \subseteq \langle a^k \rangle$

As $G = \langle a \rangle$, therefore $G \subseteq \langle a^k \rangle$.

Also, $\langle a^k \rangle \subseteq G$. Thus, $G = \langle a^k \rangle$.

Corollary 3.2: An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if gcd (k, n) = 1.

Proof: Since $G = \mathbb{Z}_n = \langle 1 \rangle$, therefore, by the theorem,

$G = \langle 1 \cdot k \rangle = \langle k \rangle$ if and only if gcd(k, n) = 1.

Problem 3.3 If $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$ be cyclic groups of orders 6, 8 and 20 respectively, find all the generators of $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$.

Solution We know that, if $G = \langle a \rangle$ be a cyclic group of order n, then $G = \langle a^k \rangle$ if and only if gcd(k, n) = 1.

Therefore generators for $\langle a \rangle$ are a, a^3, a^5. Similarly generators for $\langle b \rangle$ are b, b^3, b^5, b^7 and generators for $\langle c \rangle$ are c, c^3, c^7, c^{11}, c^{13}, c^{17}, c^{19}.

Problem 3.4 Show that if a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Solution Let $G = \langle a \rangle$.

Then each element $x \in G$ can be expressed as $x = a^n$, for some integer n.

We have $x = a^n = (a^{-1})^m$, $m = -n$ is an integer.

The above expression holds for each $x \in G$.

Hence, $G = \langle a^{-1} \rangle$.

3.3 Subgroups of Cyclic Groups

The next theorem tells us how many subgroups a finite cyclic group has and how to find them.

THEOREM 3.5:

(i) Every subgroup of a cyclic group is cyclic.

(ii) If $o(\langle a\rangle) = n$, then order of any subgroup of $\langle a\rangle$ is a divisor of n.

(iii) For each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k}\rangle$.

Proof:

(i) Let $G = \langle a\rangle$ and let H be a subgroup of G.

To show that H is cyclic.

Case I: $H = \{e\}$, then, clearly H is cyclic.

Case II: $H \neq \{e\}$, then there exists $x \in H$ such that $x \neq e$.

Also $x \in G = \langle a\rangle$. Therefore, $x = a^t$ for some $0 \neq t \in \mathbb{Z}$.

Let m be the least positive integer such that $a^m \in H$.

We shall show that $H = \langle a^m\rangle$.

As $a^m \in H$, therefore, by closure, $\langle a^m\rangle \subseteq H$. ...(1)

To show: $H \subseteq \langle a^m\rangle$. Let $y \in H$.

Also, $y \in G = \langle a\rangle$. Thus $y = a^k$, for some $k \in \mathbb{Z}$.

Applying division algorithm to k and m, there exist $q, r \in \mathbb{Z}$ such that

$$k = mq + r,\ 0 \leq r < m. \qquad ...(2)$$

Then, $a^k = a^{mq+r}$ giving $a^r = a^k \cdot a^{-mq} \in H$.

(since $a^k = y \in H$, $(a^m)^{-q} \in H$ and by closure $a^k(a^m)^{-q} \in H$)

But m is the least positive integer such that $a^m \in H$ and $0 \leq r < m$.

Therefore, $r = 0$, i.e., $k = mq$ (by (2))

Hence, $y = a^k = a^{mq} \in \langle a^m\rangle$, implying $H \subseteq \langle a^m\rangle$. …(3)

From (1) and (3), we get $H = \langle a^m\rangle$. Therefore, H is cyclic.

The above theorem is called **Fundamental Theorem of Cyclic Groups.**

Remarks:

- If a group has a non-cyclic subgroup, then, in view of the above result, the group cannot be cyclic.
- A non-cyclic group can have cyclic subgroups.

ILLUSTRATION: Consider the group of Quaternions $\mathbb{Q}_8$.

We already know that this group is non-abelian and hence non - cyclic but it has cyclic subgroups namely,

$$\langle -1\rangle = \{1\},\ \langle -1\rangle = \{-1,\ 1\},$$
$$\langle i\rangle = \{1, -1, i, -i\} = \langle -i\rangle,$$
$$\langle j\rangle = \{1, -1, j, -j\} = \langle -j\rangle,$$
$$\langle k\rangle = \{1, -1, k, -k\} = \langle -k\rangle.$$

(ii) Let $G = \langle a\rangle$. Let $o(G) = o(\langle a\rangle) = o(a) = n$ ...(1)

Now let $H \leq G$. Then, from (i), H is also cyclic.

Let $H = \langle a^m\rangle$ for some $m \in \mathbb{Z}^+$.

Let $o(H) = o(\langle a^m\rangle) = o(a^m) = k$. ...(2)

We will show that k divides n.

Consider $(a^m)^n = (a^n)^m = e^m = e$ (by (1))

But from (2), $o(a^m) = k$, giving that k is the least positive integer such that $(a^m)^k = e$.

Thus, $k \mid n$.

(iii) Let $G = \langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and let $o(a) = n$.

Then $o(G) = o(\langle a\rangle) = o(a) = n$. ...(1)

Let k divides n and consider the subgroup $\langle a^{n/k}\rangle$.

To show: $o(a^{n/k}) = k$.

We have, $(a^{n/k})^k = a^{\frac{n}{k}\cdot k} = a^n = e$.

Also, let $(a^{n/k})^t = e$. To show: $k \mid t$.

Since, $(a^{n/k})^t = e$, we have $a^{nt/k} = e$. Thus, $n \mid \frac{nt}{k}$. (by (1))

$\Rightarrow$ $nk \mid nt$, giving $k \mid t$.

$\therefore$ $o(a^{n/k}) = k$ and hence $o(\langle a^{n/k}\rangle) = k$

Thus there exists one subgroup $\langle a^{n/k}\rangle$ of order k.

Now we show uniqueness.

Let H be another subgroup of order k.

We will show that $H = \langle a^{n/k}\rangle$.

From (i), we see that H is also cyclic, i.e., $H = \langle a^m\rangle$.

Also, $o(H) = o(a^m) = o(\langle a^m\rangle) = k = o(a^{n/k})$.

And $o(a^m) = k$ implies $a^{mk} = e$ giving that $n \mid mk$, i.e., $(n/k) \mid m$.

Thus, $m = p\left(\frac{n}{k}\right)$ for some $p \in \mathbb{Z}$.

Now $a^m = a^{p\left(\frac{n}{k}\right)} = (a^{n/k})^p \in \left\langle a^{n/k} \right\rangle$. Therefore, $\langle a^m \rangle \subseteq \langle a^{n/k} \rangle$.

Also $o(\langle a^m \rangle) = o(\langle a^{n/k} \rangle)$. Hence $\langle a^m \rangle = \langle a^{n/k} \rangle$.

Therefore, there exists a unique subgroup of G of order k.

Thus, we have proved the following:

If G is a finite cyclic group and k a positive integer such that k divides order of G, then there exists a unique subgroup of G of order k.

Corollary 3.3: Let G be a finite cyclic group. Then, the number of distinct subgroups of G is equal to the number of distinct factors of $o(G)$.

For example, consider a cyclic group of order 30, i.e., $G = \langle a \rangle$ and $o(a) = 30$.

Distinct factors of 30 are 1, 2, 3, 5, 6, 10, 15 and 30.

Therefore, G has 8 distinct subgroups given by $\langle a^{30/k} \rangle$, where k is a divisor of 30.

These are:

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{29}\}; \quad o\langle a \rangle = 30$$
$$\langle a^2 \rangle = \{e, a^2, a^4, \ldots, a^{28}\}; \quad o\langle a^2 \rangle = 15$$
$$\langle a^3 \rangle = \{e, a^3, a^6, \ldots, a^{27}\}; \quad o\langle a^3 \rangle = 10$$
$$\langle a^5 \rangle = \{e, a^5, a^{10}, \ldots, a^{25}\}; \quad o\langle a^5 \rangle = 5$$
$$\langle a^6 \rangle = \{e, a^6, a^{12}, \ldots, a^{24}\}; \quad o\langle a^6 \rangle = 5$$
$$\langle a^{10} \rangle = \{e, a^{10}, a^{20}\}; \quad o\langle a^{10} \rangle = 3$$
$$\langle a^{15} \rangle = \{e, a^{15}\}; \quad o\langle a^{15} \rangle = 2$$
$$\langle a^{30} \rangle = \{e\}; \quad o\langle a^{30} \rangle = 1.$$

Corollary 3.4: For each positive divisor k of n, the set $\langle n/k \rangle$ is the subgroup of $\mathbb{Z}_n$ of order k.

(It is unique and these are the only subgroups of $\mathbb{Z}_n$)

The list of subgroups of $\mathbb{Z}_{30}$ is

$$\langle 1 \rangle = \{0, 1, 2, \ldots, 30\}; \quad o\langle 1 \rangle = 30$$
$$\langle 2 \rangle = \{0, 2, 4, \ldots, 28\}; \quad o\langle 2 \rangle = 15$$
$$\langle 3 \rangle = \{0, 3, 6, \ldots, 27\}; \quad o\langle 3 \rangle = 10$$
$$\langle 5 \rangle = \{0, 5, 10, \ldots, 25\}; \quad o\langle 5 \rangle = 6$$
$$\langle 6 \rangle = \{0, 6, 12, \ldots, 24\}; \quad o\langle 6 \rangle = 5$$

$$\langle 10\rangle = \{0, 10, 20\}; \qquad o\langle 15\rangle = 2$$
$$\langle 30\rangle = \{0\}; \qquad o\langle 30\rangle = 1.$$

Note that if k/n, then $\langle a^{n/k}\rangle$ has k elements and this is the only subgroup with k elements.

Problem 3.5 Let $G = \langle a\rangle$ be a cyclic group. If $o(a) = 24$, then find a generator for $\langle a^{21}\rangle \cap \langle a^{10}\rangle$.

In general, what is a generator for the subgroup $\langle a^m\rangle \cap \langle a^n\rangle$?

Solution We have

$$\langle a^{21}\rangle = \{e, a^{21}, a^{18}, a^{15}, a^{12}, a^9, a^6, a^3\} \text{ and}$$
$$\langle a^{10}\rangle = \{e, a^{10}, a^{20}, a^6, a^{16}, a^2, a^{12}, a^{22}, a^8, a^{18}, a^4, a^{14}\}.$$

Let $$H = \langle a^{21}\rangle \cap \langle a^{10}\rangle = \{e, a^6, a^{12}, a^{18}\}.$$

Now, H being a subgroup of a cyclic group G, is itself cyclic.

Also, $H = \langle a^k\rangle$, where k is the least positive integer such that $a^k \in H$.

So, $$\langle a^{21}\rangle \cap \langle a^{10}\rangle = \langle a^6\rangle.$$

Now, the elements of $\langle a^m\rangle$ are a^k such that k is a multiple of m. Similarly, the elements of $\langle a^n\rangle$ are a^t such that t is a multiple of n. So, the elements of $\langle a^m\rangle \cap \langle a^n\rangle$ are a^r such that r is a common multiple of m and n.

So, $\langle a^m\rangle \cap \langle a^n\rangle = \langle a^p\rangle$, where p is least common multiple of m and n.

Problem 3.6 Prove that if G is a finite cyclic group and m is a positive integer such that m divides $o(G)$, then there exists a unique subgroup of G of order m.

Proof: Let $G = \langle a\rangle$ be a finite cyclic group of order n so that $a^n = e$.

Since m divides o$(G) = n$, there exists a positive integer q such that $n = mq$.

Let $H = \{a^q, a^{2q}, \ldots, a^{mq}\} = \langle a^q\rangle$, where $a^{mq} = a^n = e$.

Thus $H = \langle a^q\rangle$ is a subgroup of G of order m.

We now show that H is a unique subgroup of G of order m.

Let K be any other subgroup of G of order m. Since a subgroup of a cyclic group is cyclic, therefore K is cyclic.

Let $K = \langle b\rangle$ for some $b \in G$ such that $b^m = e$.

Since $b \in G = \langle a\rangle$, we have $b = a^k$ for some integer k.

On dividing k by q, there exists integers t and r such that

$$k = qt + r, \quad 0 \le r < q$$

Thus $$a^{mk} = a^{mqt+mr} = (a^{mq})^t \cdot a^{mr} = a^{mr}$$

Therefore $a^{mr} = a^{mk} = (a^k)^m = b^m = e$, where $0 \le mr < mq = n$.

Since n is the least positive integer such that $a^n = e$, we must have

$$mr = 0 \quad \Rightarrow \quad r = 0, \quad \text{as} \quad m \neq 0.$$

$\therefore$ $k = qt$ and so $b = a^k = a^{qt} = (a^q)^t$.

Now $b = (a^q)^t \Rightarrow b \in H = \langle a^q \rangle \Rightarrow \langle b \rangle \subseteq H \Rightarrow K \subseteq H$.

Since $o(H) = o(K)$, we have $K = H$.

Hence, H is a unique subgroup of G of order m.

PROBLEM 3.7 How many subgroups does $\mathbb{Z}_{20}$ have? List a generator for each of these subgroups.

Suppose that $G = \langle a \rangle$ and $o(a) = 20$. How many subgroups does G have? List a generator for each of these subgroups.

SOLUTION We know order of $\mathbb{Z}_{20} = 20$. Divisors of 20 are 1, 2, 4, 5, 10, 20.

Therefore, number of subgroups of $\mathbb{Z}_{20}$ are 6 and generators for each of these subgroups are $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 4 \rangle$, $\langle 5 \rangle$, $\langle 10 \rangle$, $\langle 20 \rangle$.

We have, $G = \langle a \rangle$ and $o(a) = 20$.

Therefore generators are $\langle e \rangle$, $\langle a \rangle$, $\langle a^2 \rangle$, $\langle a^4 \rangle$, $\langle a^5 \rangle$, $\langle a^{10} \rangle$, $\langle a^{20} \rangle$.

PROBLEM 3.8 Is every subgroup of $\mathbb{Z}$, the group of integers under addition, cyclic? Justify. Describe all the subgroups of $\mathbb{Z}$.

SOLUTION Since $\mathbb{Z}$ is cyclic and every subgroup of a cyclic group is cyclic, therefore, every subgroup of $\mathbb{Z}$ is cyclic.

Now $\mathbb{Z} = \langle 1 \rangle$.

If H is any subgroup of $\mathbb{Z}$, then $H = \langle m \rangle$, for some $m \in \mathbb{Z}$.

But $\langle m \rangle = m\mathbb{Z}$ and $\langle m \rangle = \langle -m \rangle$.

Hence, the only subgroups of $\mathbb{Z}$ are $m\mathbb{Z}$, where m is a non-negative integer.

PROBLEM 3.9 Find a generator for the group $\langle m \rangle \cap \langle n \rangle$, where m and n are elements of the group $\mathbb{Z}$.

SOLUTION Clearly $\langle m \rangle \cap \langle n \rangle$ is a subgroup of $\mathbb{Z}$.

Since every subgroup of a cyclic group is cyclic, therefore $\langle m \rangle \cap \langle n \rangle$ is cyclic. Let $\langle k \rangle = \langle m \rangle \cap \langle n \rangle$.

Then $k \in \langle m \rangle \cap \langle n \rangle \Rightarrow k \in \langle m \rangle$ and $k \in \langle n \rangle$.

$\Rightarrow k$ is a multiple of m as well as n.

$\Rightarrow k$ is a common multiple of m and n.

Let l be a common multiple of m and n, then

$$l \in \langle m \rangle \text{ and } l \in \langle n \rangle \quad \Rightarrow \quad l \in \langle m \rangle \cap \langle n \rangle = \langle k \rangle$$

$\Rightarrow l$ is a multiple of k, so that $k \leq l$.

Therefore $k = \text{lcm}(m, n)$.

Hence $\text{lcm}(m, n)$ is a generator of $\langle m \rangle \cap \langle n \rangle$.

The next problem tells us that given any group, if we can find an element of group whose order is same as the order of the group, then the group is cyclic. This property is very useful in cheeking if a certain group is cyclic.

PROBLEM 3.10 Show that a finite group of order n, containing an element of order n, must be cyclic.

SOLUTION: Let G be a finite group of order n.

Let $a \in G$ be such that $o(a) = n$.

Then n is the least positive integer such that $a^n = e$.

Let $$H = \langle a \rangle = \{a, a^2, a^3, \ldots, a^n = e\}.$$

Then, H is a subgroup of G and $o(H) = n$.

Since $H \subseteq G$ and $o(H) = o(G)$, therefore $G = H = \langle a \rangle$.

Hence, G is cyclic.

Working Hint: Suppose G is a finite group of order n and we are to find whether G is cyclic or not. We should find the orders of the elements of G. If we are able to find an element $a \in G$ such that $o(a) = n$, then G will be a cyclic group and a will be a generator of the group G.
Note that if G is a cyclic group of order n, then every element of order n is a generator of G.

DEFINITION 3.2: Euler φ- function†

Let $\varphi(1) = 1$ and for any integer $n > 1$, define

$\varphi(n)$ = number of positive integers less than n and relatively prime to n.

For example,

(a) $\varphi(4) = 2$, since 1, 3 are the positive integers less than 4 and relatively prime to 4.

(b) $\varphi(7) = 6$, since 1, 2, 3, 4, 5, 6 are the positive integers less than 7 and relatively prime to 7.

† Euler φ-function is also called Euler's totient function. It is a quite significant number theoretic function having a deep connection to prime numbers and the so-called order of integers.

(c) $\varphi(8) = 4$, since 1, 3, 5, 7 are the positive integers less than 8 and relatively prime to 8.

(d) $\varphi(p) = p - 1$, if p is prime.

Remarks:

- If $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\,\varphi(n)$.
- $\phi(p^n) = p^n - p^{n-1}$, p is prime, $n \geq 1$.
- By definition, we have $o(U_n) = \varphi(n)$.

Theorem 3.6: Number of generators of a finite cyclic group of order n is $\varphi(n)$.

In other words, if $G = \langle a \rangle$ be a cyclic group of order n, then, $G = \langle a^k \rangle$ if $\gcd(k, n) = 1$.

The proof of the above theorem has already been discussed earlier.

Problem 3.11 Given the fact that $U(49)$ is cyclic and has 42 elements, deduce the number of generators that $U(49)$ has without actually finding any of the generators.

Solution We know that the number of generators of a finite cyclic group of order 42 is $\varphi(42)$, the order of $U(42)$.

Since $U(42) = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}$, therefore $o(U(42)) = 12$.

Hence, $U(49)$ has 12 generators.

We can do it other way also, as

$$\varphi(42) = \varphi(6)\,\varphi(7) = \varphi(2)\,\varphi(3)\,\varphi(7) = 1 \cdot 2 \cdot 6 = 12.$$

Theorem 3.7: If m is a positive divisor of n, then the number of elements of order m in a cyclic group of order n is $\phi(m)$.

Proof: As $m \mid n$, there exists exactly one subgroup H of G such that $o(H) = m$. Since G is cyclic, therefore H is also cyclic.

Let $H = \langle b \rangle$. Then $m = o(H) = o(b)$

So, the number of elements of order m in H equals the number of generators of H. But the number of generators of H is $\varphi(m)$, so, the number of elements of order m in H is $\varphi(m)$.

Let $k \in G$ be such that $o(k) = m$, then $K = \langle k \rangle$ has order m.

Since G has unique subgroup H of order m, therefore, $K = H$.

Therefore, $k \in H$ and so all elements of order m belong to H.

Therefore, total number of elements of order m in G is $\varphi(m)$.

Theorem 3.8: Show that the number of generators of an infinite cyclic group is two.

Proof: Let $G = \langle a \rangle$ be any infinite cyclic group.

$\therefore$ $$G = \{a^i \mid i = 0, \pm 1, \pm 2, \ldots\}$$

Since G is infinite, therefore

$$a^i = e \quad \Leftrightarrow \quad i = 0 \qquad ...(1)$$

Suppose $b \in G$ be any other generator of G so that $G = \langle b \rangle$.

Since $b \in G = \langle a \rangle$, $b = a^n$ for some integer n.

Also, since $a \in G = \langle b \rangle$, $a = b^m$ for some integer m.

$\therefore \qquad a = (a^n)^m = a^{nm}$

Now $\quad a = a^{nm} \quad \Rightarrow \quad a^{nm-1} = e \quad \Rightarrow \quad nm - 1 = 0$, using (1).

$\Rightarrow \qquad nm = 1 \quad \Rightarrow \quad n = 1, m = 1$ or $n = -1, m = -1$

$\therefore \qquad b = a \quad$ or $\quad b = a^{-1}$

Hence G has exactly two generators a and a^{-1}.

Theorem 3.9: Every non-identity element in an infinite cyclic group is of infinite order.

Proof: Let G be an infinite cyclic group generated by a, i.e., $G = \langle a \rangle$.

Clearly $o(a)$ is infinite.

Let x be a non-identity element of the group G. Then $x = a^k$, $k(\neq 0) \in \mathbb{Z}$.

Suppose, if possible, $o(a^k)$ is finite.

$\Rightarrow \quad (a^k)^m = e$ for some integer $m > 0$.

$\Rightarrow \quad a^{km} = e$

$\Rightarrow \quad o(a)$ is finite, a contradiction.

Hence the order of every non-identity element is infinite.

Problem 3.12 Let G be a group and $a, b \in G$. If $o(a) = m$, $o(b) = n$ and $\gcd(m, n) = 1$, then show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Solution Clearly $e \in \langle a \rangle$ and $e \in \langle b \rangle$.

Therefore $\qquad \{e\} \subseteq \langle a \rangle \cap \langle b \rangle \qquad ...(1)$

Let $\qquad x \in \langle a \rangle \cap \langle b \rangle$. We will show that $x = e$.

Now $\quad x \in \langle a \rangle \cap \langle b \rangle \quad \Rightarrow \quad x \in \langle a \rangle$ and $x \in \langle b \rangle$.

Thus $\quad x = a^\alpha \quad$ and $x = b^\lambda$ for some $\alpha, \lambda \in \mathbb{Z}$.

Also $\gcd(m, n) = 1$ implying $1 = mp + qn$ for some $p, q \in \mathbb{Z}$.

Thus $\qquad x = x^1 = x^{pm+qn} = x^{mp} \cdot x^{nq} = (a^\alpha)^{mp} (b^\lambda)^{nq} = (a^m)^{\alpha p} (b^n)^{\lambda q} = e$.

Therefore $\quad x \in \{e\}$ and so $\langle a \rangle \cap \langle b \rangle \subseteq \{e\} \qquad ...(2)$

Hence, from (1) and (2), we get $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Problem 3.13 Let G be a cyclic group generated by a and let $o(a) = 24$. List all generators for the subgroups of order 8.

Solution We have, $G = \langle a \rangle$ and $o(a) = 24$.

Let $H = \langle a^r \rangle$ be a subgroup of G such that $o(H) = 8$. Then $o(a^r) = 8$.

Therefore $o(a^r) = \dfrac{24}{\gcd(r, 24)}$ gives $\gcd(r, 24) = 3$.

Thus $r = 3, 9, 15, 21$ and hence generators are a^3, a^9, a^{15}, a^{21}.

Problem 3.14 If $o(a) = n$ then show that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

Solution Let $\gcd(n, k) = d$. Then $d|n$ and $d|k \Rightarrow k = dr$ for some integer r.

Now let $x \in \langle a^k \rangle$, then $x = (a^k)^p$ for some integer p.

So we have $x = a^{kp} = a^{drp} = (a^d)^{rp} \in \langle a^d \rangle$.

Therefore $\langle a^k \rangle \subseteq \langle a^d \rangle$.

Also since $\gcd(n, k) = d$, there exist $p, q \in \mathbb{Z}$ such that $np + kq = d$.

Then $a^d = a^{np+kq} = a^{np} \cdot a^{kq} = (a^n)^p \cdot (a^k)^q = e^p \cdot (a^k)^q = (a^k)^q$.

Therefore $a^d \in \langle a^k \rangle$, so that $\langle a^d \rangle \subseteq \langle a^k \rangle$

Hence we get $\langle a^k \rangle = \langle a^d \rangle = \langle a^{\gcd(n,k)} \rangle$.

Problem 3.15 Show that the group of positive rational numbers under multiplication is not cyclic.

Solution Let, if possible, $\mathbb{Q}^+$ be cyclic and let $\mathbb{Q}^+ = \langle p/q \rangle$, where $\gcd(p, q) = 1$.

Since $2 \in \langle p/q \rangle$, we have $2 = (p/q)^n$, for some $n \neq 0, \pm 1$.

$\Rightarrow$ $p^n = 2q^n$ ...(1)

$\Rightarrow$ 2 divides p^n, as $\gcd(p, q) = 1$

$\Rightarrow$ 2 divides p.

Let $p = 2t$, for some $t \in \mathbb{Z}$.

Substituting in (1) and by the same argument as above, we get 2 divides q.

So, 2 is a common divisor of p and q, contradicting that $\gcd(p, q) = 1$.

Thus, $2 \notin \langle p/q \rangle$, so that $\mathbb{Q}^+ \neq \langle p/q \rangle$ and thus $\mathbb{Q}^+$ is not cyclic.

Problem 3.16 Suppose that a and b are group elements that commute and have orders m and n respectively. If $\langle a \rangle \cap \langle b \rangle = \{e\}$, then prove that the group contains an element whose order is the least common multiple of m and n.

Show that this need not be true if a and b do not commute.

SOLUTION Let $t = \text{lcm}(m, n)$, so that m as well as n divides t.

We shall prove that ab is an element of order t. Let $o(ab) = s$.

Consider $(ab)^t = a^t b^t$, as a and b commute.

Thus $(ab)^t = e$ as $a^t = e$ and $b^t = e$. Therefore $s \mid t$.

Moreover, $o(ab) = s$ giving $e = (ab)^s = a^s b^s$, as a and b commute.

Thus $a^s = b^{-s}$ implying $a^s, b^{-s} \in \langle a \rangle \cap \langle b \rangle = \{e\}$.

Therefore $a^s = e$ and $b^{-s} = e$ giving $a^s = e$ and $b^s = e$.

Thus m divides s and n divides s (since $o(a) = m$ and $o(b) = n$)

Hence lcm(m, n) divides s, i.e., $t \mid s$.

Therefore $o(ab) = s = t = \text{lcm}(m, n)$.

Thus, G contains an element of order lcm(m, n).

In D_4, $o(F_H) = 2$, $o(F_D) = 2$, $o(F_H F_D) = o(R_{90}) = 4 \neq \text{lcm}\ (2, 2)$.

Note that $F_H F_D \neq F_D F_H$.

PROBLEM 3.17 Prove that $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in Z \right\}$ is a cyclic subgroup of $GL(2, R)$.

SOLUTION Let $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \in H$ and $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \in H$

Then, $$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+m \\ 0 & 1 \end{bmatrix} \in H$$

and $$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \in H$$

Therefore, H is a subgroup of $GL(2, R)$

Since $$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \text{ and so on.}$$

Therefore, H is a cyclic group generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

PROBLEM 3.18 Suppose that G is a finite group with the property that every non-identity element of G has prime order. If $Z(G)$ is non-trivial, then prove that every non-identity element of G has the same order.

SOLUTION Since $Z(G)$ is non-trivial, let x be any non-identity element of $Z(G)$.

We will show that the order of every element of G is $o(x)$.

Let $g \in G$. Let $o(x) = p$ and $o(g) = q$, where both p and q are prime.

We shall show $p = q$. Suppose on the contrary, $p \neq q$.

Then, since $x \in Z(G)$ we have $xg = gx$.

Also $\gcd(o(x), o(g)) = 1$.

Hence $o(xg) = o(x)\ o(g) = pq$.

But pq is not prime, therefore our assumption that $p \neq q$ is wrong.

Hence $p = q$.

Thus $o(g) = o(x)$, $\forall g \in G$, so that every element has the same order.

PROBLEM 3.19 Prove that every proper subgroup of an infinite cyclic group is infinite.

SOLUTION Let $G = \langle a \rangle$ be an infinite cyclic group and let H be a proper subgroup of G.

Then H is cyclic and if m is the least positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.

To show: H is infinite.

Suppose H is a finite group of order p. Since a^m is a generator of H, therefore $(a^m)^p = e$ giving $a^{mp} = e$, where $mp > 0$.

Therefore $o(a)$ is finite and consequently G is finite, a contradiction to the given hypothesis.

Hence H must be an infinite cyclic subgroup of G.

PROBLEM 3.20 Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G.

SOLUTION Given that $o(G) = 25$.

Since 1, 5 and 25 divide 25 therefore if $g \in G$, then $o(g) = 1$, 5 or 25.

If $o(g) = 1$ then $g = e$ $\forall g \in G$, which is not possible as $o(G) = 25$.

If $o(g) = 5$ then $g^5 = e$ $\forall g \in G$ and if $o(g) = 25$, then G is cyclic.

Problem 3.21 Let $G = \langle a \rangle$, and let H be the smallest subgroup of G that contains a^m and a^n. Prove that $H = \langle a^{\gcd(m,n)} \rangle$.

Solution Since G is cyclic, therefore H is cyclic.

Let $H = \langle a^k \rangle$ for some positive integer k. Since $a^n \in H$ and $a^m \in H$, therefore k divides both n and m.

Hence k divides $\gcd(n, m)$. Thus $a^{\gcd(n,m)} \in H = \langle a^k \rangle$.

Hence $\langle a^{\gcd(n,m)} \rangle \subseteq H$.

Also, since $\gcd(n, m)$ divides both n and m, therefore $a^n \in \langle a^{\gcd(n,m)} \rangle$ and $a^m \in \langle a^{\gcd(n,m)} \rangle$.

But H is the smallest subgroup of G containing a^n and a^m and

$a^n, a^m \in \langle a^{\gcd(n,m)} \rangle \subseteq H$, we conclude that $H = \langle a^{\gcd(n,m)} \rangle$.

Problem 3.22 Let $G = \langle a \rangle$ be a cyclic group. Suppose that G has a finite subgroup H such that $H \neq \{e\}$. Prove that G is a finite group.

Solution Clearly H is cyclic, say, $\langle a^n \rangle$, for some positive integer n. Since H is finite and $H = \langle a^n \rangle$, so $o(\langle a^n \rangle) = o(H) = m$ is finite.

Thus $(a^n)^m = a^{nm} = e$. Hence $o(a)$ divides nm.

Thus $G = \langle a \rangle$ is a finite group.

Problem 3.23 Let G be a group containing more than 12 elements of order 13. Prove that G is never cyclic.

Solution Suppose G is cyclic. Let $a \in G$ such that $o(a) = 13$.

Hence, $\langle a \rangle$ is a finite subgroup of G. Thus, G must be finite by the previous problem.

Hence, by Theorem 3.7, there are exactly $\varphi(13) = 12$ elements in G of order 13. A contradiction.

Therefore G is never cyclic.

Exercises

1. Find all the generators of $\mathbb{Z}_6, \mathbb{Z}_8$ and $\mathbb{Z}_{20}$.
2. List the elements of the subgroups $\langle 20 \rangle$ and $\langle 10 \rangle$ in $\mathbb{Z}_{30}$.
3. List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in $\mathbb{Z}_{18}$.
4. Let G be a group and let $a \in G$. Prove that $\langle a^{-1} \rangle = \langle a \rangle$.
5. If 'a' has infinite order then find all the generators of the subgroup $\langle a^3 \rangle$
6. Give example of a noncyclic group, all of whose proper subgroups are cyclic.
7. Prove that $\mathbb{Z}_n$ has an even number of generators for $n > 2$.

8. Suppose that G is a cyclic group such that $o(G) = 48$. How many subgroups does G have?

9. Let $G = \langle a \rangle$. Find the smallest subgroup of G containing a^8 and a^{12}.

10. Let G be an infinite cyclic group. Prove that e is the only element in G of finite order.

11. Let 'a' be an element of a group and let $o(a) = 15$. Compute the order of the following elements of G.

(a) a^3, a^6, a^9, a^{12}

(b) a^5, a^{10}

(c) a^2, a^4, a^8, a^{14}

12. If $o(a) = n$, show that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle >$ and that $o(a^k) = \dfrac{n}{\gcd(n, k)}$.

13. Prove that an infinite cyclic group has infinitely many subgroups.

14. Prove that if H is a subgroup of a finite cyclic group G, then $o(H)$ divides $o(G)$.

15. Prove that if G is a finite cyclic group and x an element of G, then $o(x)$ divides $o(G)$.

16. Find all the generators of the subgroup of order 15 in $\mathbb{Z}_{45}$.

17. Prove that $U(2^n)$, $n \geq 3$ is not cyclic.

Hints to selected problems

1. $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$

$\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.

$\mathbb{Z}_{20} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle$.

2. $\langle 20 \rangle = \{20, 10, 0\}$, $\langle 10 \rangle = \{10, 20, 0\}$

3. $\langle 3 \rangle = \{3, 6, 9, 12, 15, 0\}$

$\langle 15 \rangle = \{15, 12, 9, 6, 3, 0\}$

5. We know, $\langle a \rangle = \langle a^{-1} \rangle$. Let $\langle a^3 \rangle = \langle a^{-3} \rangle = \langle b \rangle$.

Then, $b = a^{3n}$, $a^3 = b^k = a^{3nk}$ giving $3 = 3nk$ or $nk = 1$. Thus, $n = k = 1$ or $n = k = -1$. Therefore, generators of the subgroup $\langle a^3 \rangle$ are a^3 and a^{-3}.

6. $U(8)$ or D_3.

7. $x \in Z_n$ is a generator if and only if $o(x) = n$. Since $o(x) = o(x^{-1})$ and $x \neq x^{-1}$ as $o(x) = n > 2$. Therefore, generators occur in pairs.

8. Since for each positive divisor k of 48, there is a unique subgroup of order k, number of all subgroups of G equals to the number of all positive divisors of 48, i.e., 8.

10. Since G is an infinite cyclic group, $G = \langle a \rangle$ for some $a \in G$ such that $o(a)$ is infinite. Now, assume that there is an element $b \in G$ such that $o(b) = m$ and $b \neq e$. Since $G = \langle a \rangle$, $b = a^k$ for some $k \geq 1$. Hence, $e = b^m = (a^k)^m = a^{km}$. Hence, o($a$) divides km, a contradiction, since $o(a)$ is infinite. Thus, e is the only element in G of finite order.

11. (*a*) $o(a^3) = \dfrac{o(a)}{\gcd(3, o(a))} = \dfrac{15}{\gcd(3,15)} = \dfrac{15}{3} = 5$

Similarly $o(a^6) = o(a^9) = o(a^{12}) = 5$.

(b) $o(a^5) = \dfrac{o(a)}{\gcd(5, o(a))} = \dfrac{15}{\gcd(5,15)} = \dfrac{15}{5} = 3$

Similarly, $o(a^{10}) = 3$

(c) $o(a^2) = \dfrac{o(a)}{\gcd(2, o(a))} = \dfrac{15}{\gcd(2,15)} = \dfrac{15}{1} = 15$

Similarly, $o(a^4) = o(a^8) = o(a^{14}) = 15$.

12. Let $\gcd(n, k) = d$.

Then d/n and $d/k \Rightarrow k = dr$ for some integer r.

Let $x \in \langle a^k \rangle \Rightarrow x = (a^k)^p$ for some integer p.

So, we have $x = a^{kp} = a^{drp} = (a^d)^{rp} \in \langle a^d \rangle$.

$\therefore \quad \langle a^k \rangle \subseteq \langle a^d \rangle$.

Also, since $\gcd(n, k) = d$, there exist integers p, q such that $np + kq = 1$.

Now, $a^d = a^{np+kq} = a^{np} \cdot a^{kq} = (a^n)^p \cdot (a^k)^q = e^p \cdot (a^k)^q = (a^k)^q$.

Therefore, $a^d \in \langle a^k \rangle$, so that $\langle a^d \rangle \subseteq \langle a^k \rangle$

Hence, we get $\langle a^k \rangle = \langle a^d \rangle = \langle a^{\gcd(n,k)} \rangle$.

Second part already done.

14. Let $G = \langle a \rangle$ be a finite cyclic group of order n. Let H be a subgroup of G.

Then, H, being a subgroup of a cyclic group, is cyclic.

Let $H = \langle a^k \rangle$, where $k \in \mathbb{Z}$, $0 < k < n$. Then, $o(H) = o(a^k)$.

But $(a^k)^n = a^{kn} = (a^n)^k = e$, therefore, $o(a^k)$ divides n, i.e., $o(H)$ divides $o(G)$.

❑❑❑

4

Permutation Groups

Learning Objectives

- Permutation of a Set
- Permutation Group of a Set
- Cycle Notation for a Permutation
- Theorems on Permutations and Cycles.
- Even and Odd Permutations

4.1 Permutation of a Set

Permutations of finite sets are used in every branch of mathematics—for example, in geometry, in statistics, in elementary algebra, and they have numerous applications in science and technology. Even in puzzles like Rubik's Cube†, permutation groups are used to show its multiple solutions. The different alterations and alignments of the cube, form a subgroup of a permutation group, obtained from the different horizontal and vertical rotations of the puzzle.

Because of their practical importance, this chapter is devoted to the study of a few special properties of permutations of finite sets.

We define a permutation in Algebra as follows.

† Rubik's Cube is a three dimensional combination puzzle (see figure on the cover page of the book), invented in the year 1974 by Hungarian inventor, architect and professor of architecture, Ern¨o Rubik. The cube was first launched to the public in the year 1980 and quickly became popular. Over the years, 350 million cubes have been sold, becoming one of the best selling puzzles.
David Breyer Singmaster, an American mathematics professor at London South Bank University in the United Kingdom, in his notes on *Rubik's* "*Magic Cube*", provided the first mathematical introduction to the Cube. He also introduced 'Singmaster Notation' for the different rotations of the cube. Today, several methods for solving the cube exist.

© The Author(s) 2023

D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_4

Definition 4.1: Let A be any set. Then, a function $\alpha : A \to A$ is called a **permutation of the set A** if and only if α is one-one and onto.

So, by a permutation of a set A, we mean a bijective function from A to A, that is, a one-to-one correspondence between A and itself.

We confine ourselves to the case when A is a finite set.

For example, we define a permutation α of the set $\{1, 2, 3, 4\}$ by specifying

$$\alpha(1) = 3, \quad \alpha(2) = 2, \quad \alpha(3) = 4, \quad \alpha(4) = 1.$$

A more convenient way to express this correspondence is to write α in array form as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}.$$

Here the elements of the set A are written in the first row and we write the image of every element just below it. It is immaterial in which order the elements of A are put in the first row. This is the **two-row notation** for writing a permutation.

Similarly, the permutation β of the set $\{1, 2, 3, 4, 5\}$ given by

$$\beta(1) = 4, \quad \beta(2) = 5, \quad \beta(3) = 1, \quad \beta(4) = 2, \quad \beta(5) = 3$$

is expressed in the two-row notation as

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{bmatrix}$$

Definition 4.2: For the permutations expressed in two-row notation, **the product or the composition of these permutations** is carried out by moving from right to left with going from top to bottom, then again from top to bottom.

For example, let

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} \quad \text{and} \quad \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$$

then

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

We have 4 under 1, since $(\gamma\sigma)(1) = \gamma(\sigma(1)) = \gamma(2) = 4$, so $\gamma\sigma$ sends 1 to 4.

The remainder of the bottom row of $\gamma\sigma$ is obtained in a similar fashion.

Definition 4.3: For any set A, define $I : A \to A$ as $I(x) = x, \ \forall x \in A$.

I is called **identity permutation.**

For example, let $A = \{1, 2, 3, 4\}$. Then, the identity map on A is

$$I = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}$$

Since a permutation on a set A is a one-one, onto map, so its inverse must exist.

Let us illustrate by an example how to find the **inverse of a permutation** in a two-row notation.

Consider the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$

The inverse of α is a permutation β such that $\alpha\beta = \beta\alpha = I$.

Note that if we take $\beta = \begin{bmatrix} 2 & 4 & 3 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$

Then, $\alpha\beta = \beta\alpha = I$.

Thus the inverse of a permutation is obtained just by interchanging the rows of the permutation and then in the top row we write the elements in the order 1, 2, 3, ..., n, so we get

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{bmatrix}$$

This leads us to the following definition of the **inverse of a permutation:**

Definition 4.4: For any set A, define $\sigma^{-1} : A \to A$ as $\sigma^{-1}(i) = j$ if and only if $\sigma(j) = i$.

Then, σ^{-1} is the **inverse of the permutation** σ.

4.2 Permutation Group of a Set

A permutation group is a set of permutations that forms a group under the operation of function composition. Permutation groups have several applications. Some of these are specific to higher level mathematics courses, while many can be applied to real world problems. They are also used to show the multiple solutions of the Rubik's Cube. In fact, solving Rubik's cube has become a major area of study for many people. Rubik's cube enthusiasts have discovered a general algorithm for restoring the cube to the start position from the scrambled state using permutation groups.

Definition 4.5: A **permutation group** of a set A is a set of permutations of A that forms a group under function composition, i.e., $(\alpha \circ \beta)(x) = \alpha(\beta(x))$ for all $x \in A$.

In other words, a permutation group of a set A is a set of those one-one onto mappings from A to A that forms a group under function composition.

$\alpha \circ \beta$ in short is denoted by $\alpha\beta$.

Definition 4.6: Let $A = \{1, 2, 3, ..., n\}$. The set of all permutations of A is called **the symmetric group of degree *n*** and is denoted by S_n.

Elements of S_n have the form: $\sigma = \begin{bmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{bmatrix}$

Remarks:

- $o(S_n) = n!$

As there are n choices for $\sigma(1)$. Once we determine $\sigma(1)$, then since σ is one to one, we have $\sigma(1) \neq \sigma(2)$ and thus there are only $(n - 1)$ possibilities left for $\sigma(2)$. After choosing $\sigma(2)$, there are exactly $(n - 2)$ possibilities left for $\sigma(3)$. Continuing like this, we see that S_n must have $n(n - 1) \ldots 3 \cdot 2 \cdot 1 = n!$ elements.

- For $n \geq 3$, S_n is non-abelian. As $n \geq 3$, let

$$\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \quad \text{and} \quad \tau = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

Then,
$$\sigma\tau = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

and
$$\tau\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}.$$

It can be seen that $\sigma\tau \neq \tau\sigma$.

Example 4.1: Symmetric Group S_3

Let S_3 denote the set of all one-one onto functions from $A = \{1, 2, 3\}$ to itself. As discussed earlier we have $o(S_3) = 3! = 6$.

These six elements are:

$$\alpha_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \ \alpha_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \ \alpha_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

$$\alpha_3 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \ \alpha_4 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \ \alpha_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

The composition table is

Table 4.1: Composition Table for S_3

	α_0	α_1	α_2	α_3	α_4	α_5
α_0	α_0	α_1	α_2	α_3	α_4	α_5
α_1	α_1	α_2	α_0	α_5	α_3	α_4
α_2	α_2	α_0	α_1	α_4	α_5	α_3
α_3	α_3	α_4	α_5	α_0	α_1	α_2
α_4	α_4	α_5	α_3	α_2	α_0	α_1
α_5	α_5	α_3	α_4	α_1	α_2	α_0

From the table, we see that $\alpha_i \alpha_j \in S_3$. $\forall \alpha_i, \alpha_j \in S_3$. So, closure property holds.

Also, since composition of mappings is associative, therefore associativity holds.

The permutation $\alpha_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ acts as the identity permutation.

Also, from the table, it can be observed that

$$\alpha_0^{-1} = \alpha_0,\ \alpha_1^{-1} = \alpha_2,\ \alpha_2^{-1} = \alpha_1,\ \alpha_3^{-1} = \alpha_3,\ \alpha_4^{-1} = \alpha_4,\ \alpha_5^{-1} = \alpha_5$$

Thus S_3, under function composition, forms a group with six elements.

Also, since $\alpha_1 \alpha_3 \neq \alpha_3 \alpha_1$, we have S_3 is non–abelian.

Note that the elements of S_3 can be related with the elements of the Dihedral group D_3, by identifying the vertices a, b, c of the equilateral triangle with the elements 1, 2, 3 respectively of the set A. In that case, the elements R_0, R_{120}, R_{240}, F_A, F_B, F_C of D_3 are same as the elements α_0, α_2, α_1, α_3, α_4, α_5 respectively, of S_3.

EXAMPLE 4.2: Symmetric Group (S_4)

Let S_4 denote the set of all one-one onto functions from {1, 2, 3, 4} to itself.

Then S_4, under function composition, forms a group with 4! = 24 elements.

The twenty-four elements are described as:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix},$$

Note that in the notation of permutations, the elements of D_4 can be written as

$$R_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix},\ R_{90} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix},\ R_{180} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix},$$

$$R_{270} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix},\ F_H = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix},\ F_V = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix},$$

$$F_D = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix},\ F_{D'} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix}.$$

It can be easily seen that D_4 is a subgroup of S_4.

Problem 4.1 Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}$

Compute each of the following:

(a) α^{-1} (b) $\beta\alpha$ (c) $\alpha\beta$

Solution

(a) $\alpha^{-1} = \begin{bmatrix} 2 & 1 & 3 & 5 & 4 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$

(b) $\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 4 & 5 \end{bmatrix}$

(c) $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{bmatrix}$

4.3 Cycle Notation

A cycle notation is yet another way to express a permutation.

Definition 4.7: A **cycle of length *k*** is a permutation which permutes k elements in cyclic order and remaining elements remain unchanged.

In other words, a permutation σ of a finite set A is called a cycle if there exist elements $x_1, x_2, \ldots, x_k$ in A such that $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, ..., $\sigma(x_{k-1}) = x_k$, $\sigma(x_k) = x_1$ and the other elements remain fixed under σ, i.e., $\sigma(x) = x$ for other $x \in A$.

This notation of σ is called a one-row notation.

A cycle of length k is denoted by $(x_1\ x_2\ \ldots\ x_k)$. It is also called a k-cycle.

For example:

$\sigma = \begin{bmatrix} 1 & 3 & 4 & 2 & 6 & 5 & 7 & 8 & 9 \\ 3 & 4 & 2 & 6 & 5 & 7 & 8 & 9 & 1 \end{bmatrix} = (1\,3\,4\,2\,6\,5\,7\,8\,9)$ is a cycle of length 9,

whereas $\tau = \begin{bmatrix} 1 & 3 & 5 & 7 & 2 & 4 & 6 \\ 3 & 5 & 7 & 1 & 2 & 4 & 6 \end{bmatrix} = (1\,3\,5\,7)$ is a cycle of length 4.

Remarks:

- Any missing element in the cyclic notation is mapped to itself.
  As in the above example, it is understood that $2 \to 2$, $4 \to 4$, $6 \to 6$.
  τ can also be written as $\tau = (1\ 3\ 5\ 7)(2)(4)(6)$.
- For $I \in S_n$, $I = (n)$ for any n.
  For example, $I = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$ could be written as $I = (5)$ or $I = (1)$
  and so on.
  Thus a 1-cycle is nothing but the identity permutation
- Let $\tau = (x_1\ x_2\ \ldots\ x_{m-1}\ x_m)$ be a m-cycle then $\tau^{-1} = (x_m\ x_{m-1}\ \ldots\ x_2\ x_1)$.

DEFINITION 4.8: Product of Cycles

Let us illustrate by examples, how to find the **product of cycles.**

1. Let $\alpha = (1\ 2)(3)(4\ 5)$
   and $\beta = (1\ 5\ 3)(2\ 4)$
   Then, $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix} = (1\ 4)\ (2\ 5\ 3)$
2. Let $\alpha = (1\ 3)(2\ 7)(4\ 5\ 6)(8)$
   and $\beta = (1\ 2\ 3\ 7)(6\ 4\ 8)(5)$.
   Then, $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 2 & 8 & 6 & 5 & 3 & 4 \end{bmatrix} = (1\ 7\ 3\ 2)\ (4\ 8)\ (5\ 6)$
3. If $\alpha = (1\ 2)(3)(4\ 5)$
   and $\beta = (1\ 5\ 3)(2\ 4)$
   Then, $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix} = (1\ 4)\ (2\ 5\ 3)$.

Remark: In cycle notations:

- $S_3 = \{I, (12), (13), (23), (123), (132)\}$
- $sS_4 = \{I, (12), (13), (14), (23), (24), (34), (123), (124), (132), (142), (134), (143), (234), (243), (1234), (1432), (1243), (1342), (1324), (1423), (12)(34), (13)(24), (14)(23)\}$

4.4 Theorems on Permutations and Cycles

The permutation $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 1 & 9 & 8 & 5 & 6 & 2 \end{bmatrix}$

can be written as $\sigma = (1\ 3\ 4)(2\ 7\ 5\ 9)(6\ 8)$.

Also, the permutation $g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 9 & 7 & 8 \end{bmatrix}$ can be written as

$g = (1\ 2\ 5\ 6)(3\ 4)(7\ 9\ 8)$.

i.e., every permutation can be written as product of disjoint cycles (i.e., these cycles have no element in common).

We now prove the following theorem:

Theorem 4.1: Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Proof: Let $A = \{1, 2, ..., n\}$ and let α be a permutation on A.

If $\alpha = I$, then we are done. Now let $\alpha \neq I$.

Consider any element of A, say a_1.

Let $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$, i.e., $\alpha^2(a_1) = a_3$,

$\vdots \quad \vdots \quad \vdots$

In general, we have $\alpha^k(a_1) = a_{k+1}$. ...(1)

As A is finite, the sequence $\alpha(a_1)$, $\alpha^2(a_1)$, ... must have finite distinct elements, for if $\alpha^i(a_1) = \alpha^j(a_1)$ for some $i \neq j$, say, $j > i$.

Then $\alpha^{j-i}(a_1) = a_1$. Let $m = j - i$, then $\alpha^m(a_1) = a_1$.

Hence, distinct elements in the above sequence are

$$a_1, \alpha(a_1), \alpha^2(a_1), \ldots, \alpha^{m-1}(a_1) \qquad (\because \alpha^m(a_1) = a_1)$$

By notation in (1), $a_1, a_2, a_3, \ldots, a_m$ are distinct elements of A obtained by this process.

If $\alpha = (a_1 a_2 \ldots a_m)$ we are done, else choose $b_1 \notin (a_1 a_2 \ldots a_m)$ ...(2)

Again, let $b_2 = \alpha(b_1)$, $b_3 = \alpha^2(b_1)$ and so on.

Again, as A is finite, $b_1 = a^k(b_1)$ for some k. Also, elements in $(b_1 b_2 \ldots b_k)$ have no elements common to $(a_1 a_2 \ldots a_m)$, as if $\alpha^i(a_1) = \alpha^j(b_1)$, then $\alpha^{i-j}(a_1) = b_1$. This gives $b_1 = a_t$ for some t, which is a contradiction (by (2)).

Continuing like this until all the elements of A are used, we get

$$\alpha = (a_1 a_2 \ldots a_m)(b_1 b_2 \ldots b_k) \ldots (c_1 c_2 \ldots c_s)$$

In this way every permutation can be written as a product of disjoint cycles.

Consider the two disjoint cycles

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 7 & 4 & 5 & 6 & 2 \end{bmatrix} = (1\,3\,7\,2)$$

and $$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 6 & 4 & 5 & 7 \end{bmatrix} = (4\,6\,5)$$

Then $$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 7 & 4 & 5 & 6 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 6 & 4 & 5 & 7 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 7 & 6 & 4 & 5 & 2 \end{bmatrix} = (1\,3\,7\,2)\,(4\,6\,5)$$

and $$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 6 & 4 & 5 & 7 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 7 & 4 & 5 & 6 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 7 & 6 & 4 & 5 & 2 \end{bmatrix} = (1\,3\,7\,2)\,(4\,6\,5)$$

$\therefore\ \alpha\beta = \beta\alpha$, i.e., disjoint cycles commute.

We now prove the following theorem showing that disjoint cycles commute.

THEOREM 4.2: If the pair of cycles $\alpha = (a_1 a_2 \ldots a_m)$ and $\beta = (b_1 b_2 \ldots b_n)$ have no entries in common, then they commute.

Proof: Let $\alpha = (a_1 a_2 \ldots a_m)$ and $\beta = (b_1 b_2 \ldots b_n)$ be two disjoint cycles (permutations) of the set $S = \{a_1, a_2 \ldots a_m, b_1, b_2 \ldots b_n, c_1, c_2, \ldots, c_k\}$ where c_i's are the members of S left fixed by both α and β.

To prove: $\alpha\beta = \beta\alpha$, i.e., $(\alpha\beta)(x) = (\beta\alpha)(x)$, $\forall x \in S$.

Note that $\alpha(a_i) = a_{i+1}$, for all $i = 1, 2, \ldots m-1$ and $\alpha(a_m) = a_1$ ...(1)

Also, $\alpha(b_i) = b_i, \quad \forall i = 1,2,\ldots n$ and $\alpha(c_i) = c_i, \quad \forall i = 1,2,\ldots k$

Similarly, $\beta(a_i) = a_i, \quad \forall i = 1,2,\ldots m$ and $\beta(c_i) = c_i, \quad \forall i = 1,2,\ldots k$

and $\beta(b_i) = b_{i+1}$, for all $i = 1, 2, \ldots n-1$ and $\beta(b_n) = b_1$ ...(2)

Case I: If $x = c_i$ for some $i = 1, 2, \ldots, k$ then

Consider $(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i)$ (by (2))

$= c_i$ (by (1))

Also, $(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i)$ (by (1))

$= c_i$ (by (2))

Therefore $(\alpha\beta)(c_i) = (\beta\alpha)(c_i)$, for all $i = 1, 2, \ldots, k$

Case II: If $x = a_i$ for some $i = 1, 2, \ldots, m$, then

$$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1} \qquad \text{(Using (1) and (2))}$$

Also, $(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$ (Using (1) and (2))

Thus $(\alpha\beta)(a_i) = (\beta\alpha)(a_i)$ for each $i = 1, 2, \ldots, m$.

Case III: If $x = b_i$ for some $i = 1, 2, \ldots, n$, then as discussed in case II, we get $(\alpha\beta)(b_i) = (\beta\alpha)(b_i)$.

Hence, in all cases $(\alpha\beta)(x) = (\beta\alpha)(x), \quad \forall x \in S$.

Thus, $\alpha\beta = \beta\alpha$, i.e., disjoint cycles commute.

Consider the cycle $\alpha = (1\ 2\ 3)$.

Then, $\alpha(1) = 2, \quad \alpha(2) = 3, \quad \alpha(3) = 1.$

Now, $\alpha(1) = 2, \quad \alpha^2(1) = 3, \quad \alpha^3(1) = 1$

$\alpha(2) = 3, \quad \alpha^2(2) = 1, \quad \alpha^3(2) = 2$

$\alpha(3) = 1, \quad \alpha^2(3) = 2, \quad \alpha^3(3) = 3.$

So, $\alpha^3(a_i) = a_i \quad \forall\, i = 1,2,3.$ Thus, $\alpha^3 = I$.

Therefore, $o(\alpha) = 3$.

Also, α is a cycle of length 3.

So, we note that a cycle of length 3 has order 3. We now generalize this result.

LEMMA 4.1: If $\alpha = (a_1\ a_2\ \ldots\ a_n)$ be a cycle of length n, then $o(\alpha) = n$.

Proof:

Let $$\alpha = (a_1\ a_2 \ldots a_n) = \begin{bmatrix} a_1 & a_2 & \ldots & a_n & b_1 & \ldots & b_m \\ a_2 & a_3 & \ldots & a_1 & b_1 & \ldots & b_m \end{bmatrix},$$

i.e., let α be the permutation of the set $\{a_1, a_2, \ldots, a_n, b_1, \ldots, b_m\}$.

Consider

$$\alpha^2 = \begin{bmatrix} a_1 & a_2 & \ldots & a_n & b_1 & \ldots & b_m \\ a_2 & a_3 & \ldots & a_1 & b_1 & \ldots & b_m \end{bmatrix} \begin{bmatrix} a_1 & a_2 & \ldots & a_n & b_1 & b_2 & \ldots & b_m \\ a_2 & a_3 & \ldots & a_1 & b_1 & b_2 & \ldots & b_m \end{bmatrix}$$

$$= \begin{bmatrix} a_1 & a_2 & \ldots & a_n & b_1 & b_2 & \ldots & b_m \\ a_3 & a_4 & \ldots & a_2 & b_1 & b_2 & \ldots & b_m \end{bmatrix}$$

i.e., α^2 moves every symbol two places along right side.

Similarly, $\alpha^3 = \begin{bmatrix} a_1 & a_2 & \ldots & a_n & b_1 & \ldots & b_m \\ a_4 & a_5 & \ldots & a_3 & b_1 & \ldots & b_m \end{bmatrix}$ moves every symbol three places along right side.

Continue like this, we see that $\alpha^n = \begin{bmatrix} a_1 & a_2 & \ldots & a_n & b_1 & \ldots & b_m \\ a_1 & a_2 & \ldots & a_n & b_1 & \ldots & b_m \end{bmatrix} = I$

Therefore $o(\alpha) = n$. Hence, a cycle of length n has order n.

THEOREM 4.3: The **order of a permutation** of a finite set written in disjoint cycles form is the least common multiple of the lengths of the cycles.

Proof: Let $\sigma = \alpha\beta$, where α and β are disjoint cycles.

Let $\alpha = (a_1\ a_2\ ...\ a_m)$ and $\beta = (b_1\ b_2\ ...\ b_n)$.

Then, α has length m and β has length n.

Therefore, by Lemma 4.1, $o(\alpha) = m$ and $o(\beta) = n$. ...(1)

Let $k = \text{lcm}(m, n)$. To prove: $o(\sigma) = k$.

Let $o(\sigma) = t$. We need to show that $k = t$.

As $k = \text{lcm}(m, n)$, therefore $m|k$ and $n|k$.

Thus, $k = am$ for some $a \in \mathbb{Z}$ and $k = bn$ for some $b \in \mathbb{Z}$.

Consider, $\alpha^k = \alpha^{am} = (\alpha^m)^a = I$, as $o(\alpha) = m$.

Similarly, we have $\beta^k = I$.

Therefore, since α and β are disjoint, we have $\sigma^k = (\alpha\beta)^k = \alpha^k \beta^k = I$

But we know $o(\sigma) = t$, therefore $t|k$. ...(A)

As $o(\sigma) = t$, we have $\sigma^t = I$, implying $(\alpha\beta)^t = I$, i.e., $\alpha^t \beta^t = I$

But as α and β are disjoint, so are α^t and β^t (since raising a power on permutation does not introduce new symbol)

Therefore, $\alpha^t = I$ and $\beta^t = I$. This gives $m|t$ and $n|t$.

Thus, $\text{lcm}(m, n)|t$, implying that $k|t$ ...(B)

Therefore, from (*A*) and (*B*), we conclude that $k = t$.

Now let $\sigma = \alpha_1\alpha_2 ... \alpha_n$ be the representation of σ as a product of disjoint cycles $\alpha_1, \alpha_2, ..., \alpha_n$.

Let for each $i = 1, 2, ... , n$, $o(\alpha_i) = k_i$ and let $k = \text{lcm}(k_1, k_2, ... , k_n)$. Then, for all i, $k_i|k$ and thus $k = r_i k_i$ for $r_i \in \mathbb{Z}$.

We will show that $o(\sigma) = k$.

Firstly, since disjoint cycles commute, we have

$$\sigma^k = \left(\alpha_1\alpha_2 \ldots \alpha_n\right)^k = {\alpha_1}^k {\alpha_2}^k \ldots {\alpha_n}^k = {\alpha_1}^{r_1 k_1} {\alpha_2}^{r_2 k_2} \ldots {\alpha_n}^{r_n k_n} = I$$

Now suppose that $\sigma^t = I$ for some t. Then, $(\alpha_1\ \alpha_2\ ...\ \alpha_n)^t = I$.

This implies ${\alpha_1}^t {\alpha_2}^t\ ...\ {\alpha_n}^t = I$ and thus each ${\alpha_i}^t = I$.

Now, since $o(\alpha_i) = k_i$, we have $r_i|t$. This gives that $k|t$.

Therefore, $o(\sigma) = k = \text{lcm}(o(\alpha_1), o(\alpha_2), ... , o(\alpha_n))$.

Hence, order of a permutation written as a product of two (or more) disjoint cycles is the lcm of the lengths of the cycles.

PROBLEM 4.2 What is the order of each of the following permutations?

(a) $\alpha = (1\ 2\ 4)(3\ 5\ 7)$,

(b) $\beta = (1\ 2\ 4)(3\ 5)$,

(c) $\gamma = (1\ 2\ 4)(3\ 5\ 7\ 8)$.

SOLUTION

(a) $o(\alpha) = \text{lcm}(3, 3) = 3$

(b) $o(\beta) = \text{lcm}(3, 2) = 6$

(c) $o(\gamma) = \text{lcm}(3, 4) = 12$.

PROBLEM 4.3 What is the order of each of the following permutations?

(a) $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}$

(b) $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}$.

SOLUTION

(a) We can write $\alpha = (1\ 2)(3\ 5\ 6)(4)$.

Thus, $o(\alpha) = \text{lcm}(2, 3, 1) = 6$.

(b) Here, $\beta = (1\ 7\ 5\ 3)(2\ 6\ 4)$.

Therefore, $o(\beta) = \text{lcm}(4, 3) = 12$.

PROBLEM 4.4 What is the order of the product of a pair of disjoint cycles of lengths 4 and 6?

SOLUTION

Since a cycle of length n has order n, therefore the order of the product is given by $\text{lcm}(4, 6) = 12$.

PROBLEM 4.5 Let $\beta = (1\ 3\ 5\ 7\ 9\ 8\ 6)(2\ 4\ 10)$. What is the smallest positive integer n for which $\beta^n = \beta^{-5}$?

SOLUTION

Since $o(\beta) = \text{lcm}(7, 3) = 21$. Therefore, $\beta^{21} = I$ and so $\beta^{16} = \beta^{-5}$.

PROBLEM 4.6 Let $H = \{\beta \in S_5 : \beta(1) = 1 \quad \text{and} \quad \beta(3) = 3\}$.
Prove that H is a subgroup of S_5.

SOLUTION

$H \neq \phi$ as $I(1) = 1$ and $I(3) = 3$, so $I \in H$.

Now, let $\alpha, \beta \in H$ then $\alpha(1) = 1$, $\alpha(3) = 3$, $\beta(1) = 1$ and $\beta(3) = 3$. ...(1)

Therefore $\alpha\beta(1) = \alpha(\beta(1)) = \alpha(1) = 1$ and $\alpha\beta(3) = \alpha(\beta(3)) = \alpha(3) = 3$

Hence, $\alpha\beta \in H$.

Also, from (1), we have $\alpha^{-1}(1) = 1$ and $\alpha^{-1}(3) = 3$.

So, $\alpha^{-1} \in H$ for $\alpha \in H$ and therefore $H \leq S_5$.

PROBLEM 4.7 Let $\alpha = (1\ 3\ 5\ 7\ 9)(2\ 4\ 6)\ (8\ 10)$. If α^m is a 5-cycle, what can you say about m?

SOLUTION

We have, $o(\alpha) = \text{lcm}(2, 3, 5) = 30$. Thus, $o(\alpha) = 30$.

This gives us $\alpha^{30} = I$ implying $(\alpha^6)^5 = I$, i.e., $o(\alpha^6) = 5$.

Therefore, α^6 is a 5-cycle and hence m is 6.

DEFINITION 4.9: A cycle of length 2 is known as a **transposition** or a **2-cycle.**

Consider a permutation written in cycle form as (1 2 3 4 5).

We can write this permutation in the form (1 5)(1 4)(1 3)(1 2), as product of two cycles.

So, we have the following theorem:

THEOREM 4.4: Every permutation in S_n, $n > 1$ can be expressed as a product of transpositions.

Proof: We know that identity permutation can be written as $I = (12)(12)$, which is product of transpositions.

Now, let α be a permutation in S_n $(n > 1)$ such that $\alpha \neq I$.

Suppose $\alpha = (a_1\ a_2 \ldots a_k)(b_1\ b_2 \ldots b_m)(c_1\ c_2 \ldots c_n)$

By direct computation, we get

$$(a_1 a_2 \ldots . a_k) = (a_1 a_k)(a_1 a_{k-1}) \ldots . (a_1 a_2) \text{ and so on.}$$

Therefore, we can write α as

$$\alpha = (a_1 a_k)(a_1 a_{k-1}) \ldots (a_1 a_2)(b_1 b_m)(b_1 b_{m-1}) \ldots (b_1 b_2)(c_1 c_n)(c_1 c_{n-1}) \ldots (c_1 c_2)$$

Thus, every permutation in S_n, $n > 1$ can be written as a product of 2-cycles.

Remark: Note that the decomposition of a cycle as a product of 2-cycles is not unique.

For example, we can write

$$\begin{aligned}(1\ 2\ 3\ 4\ 5) &= (1\ 5)(1\ 4)(1\ 3)(1\ 2)\\ &= (4\ 5)(5\ 3)(2\ 5)(1\ 5)\\ &= (2\ 1)(2\ 5)(2\ 4)(2\ 3)\\ &= (5\ 4)(5\ 2)(2\ 1)(2\ 5)(2\ 3)(1\ 3)\end{aligned}$$

Problem 4.8 Let $\alpha = \begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 2 & 1 & 3 & 5 & 4 & 7 & 6 & 8\end{bmatrix}$ and

$$\beta = \begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4\end{bmatrix}$$

Write α and β as

(a) product of disjoint cycles

(b) product of 2-cycles

Solution

(a) $\alpha = (1\ 2)(3)(4\ 5)(6\ 7)(8)$ and $\beta = (1)(2\ 3\ 8\ 4\ 7)(5\ 6)$

(b) $\alpha = (1\ 2)(4\ 5)(6\ 7)$ and $\beta = (2\ 7)(2\ 4)(2\ 8)(2\ 3)(5\ 6)$

Lemma 4.3: In S_n, there are $\frac{1}{r}\frac{n!}{(n-r)!}$ distinct cycles of length $r (r \le n)$.

Proof: The number of distinct arrangements of r numbers out of n numbers is given by ${}^{n}p_r = \frac{n!}{(n-r)!}$.

Since the cycles (1 2 3 .... r), (2 3 .... r 1), ... (r 1 2 ... $r-1$), which are r in number, are same.

Therefore, total number of distinct cycles of length r is equal to

$$\frac{1}{r}\frac{n!}{(n-r)!} = {}^{n}C_r (r-1)!$$

Problem 4.9 In S_4, find a cyclic group and a non-cyclic group of order 4.

Solution Let $H = \{I, (12)(34), (14)(23), (13)(24)\}$

Then H is a non-cyclic subgroup of S_4 of order 4 and let

$$\begin{aligned}K &= \{I, (1234), (1234)^2, (1234)^3\}\\ &= \{I, (1234), (13)(24), (1432)\} = \langle(1234)\rangle.\end{aligned}$$

Then K is a cyclic subgroup of S_4 of order 4.

PROBLEM 4.10 Suppose that β is a 10-cycle. For which integers i, between 2 and 10, is β^i also a 10-cycle?

SOLUTION

Let β = (1 2 3 4 5 6 7 8 9 10). Then

β^2 = (1 2 3 5 6 7 8 9 10)(1 2 3 4 5 6 7 8 9 10) = (1 3 5 7 9)(2 4 6 8 10)

β^3 = (1 3 5 7 9)(2 4 6 8 10)(1 2 3 4 5 6 7 8 9 10) = (1 4 7 10 3 6 9 2 5 8)

β^5 = (1 6)(2 7)(3 8)(4 9)(5 10) and so on.

Note that β^3, β^7, β^9 are 10-cycles.

Another solution:

We know that if $a \in G$, then $o(a^n) = \dfrac{o(a)}{\gcd(n, o(a))}$.

Let $a = \beta$, $n = i$. Then, we have $o(\beta^i) = \dfrac{o(\beta)}{\gcd(i, o(\beta))}$

If $o(\beta^i) = 10$, then $10 = \dfrac{10}{\gcd(i,10)}$, implying $\gcd(i, 10) = 1$.

Thus, $i = 3, 7, 9$.

PROBLEM 4.11 In S_3, find elements α and β such that $o(\alpha) = o(\beta) = 2$ and $o(\alpha\beta) = 3$.

SOLUTION Let α = (1 2), β = (1 3). Then, αβ = (1 3 2) with $o(\alpha\beta) = 3$.

PROBLEM 4.12 Let G be the set of all permutations of the positive integers. Let H be the subset of elements of G that can be expressed as a product of a finite number of cycles. Prove that H is a subgroup of G.

SOLUTION Since I = (1 2)(1 2) as product of finite number of cycles, therefore, $I \in H$ and hence $H \neq \phi$.

Let $\alpha = a_1 a_2 \ldots a_n$ and $\beta = b_1 b_2 \ldots b_m$, where $a_i's$ and $b_j's$ are cycles.

Then α, β ∈ H.

Now $\alpha\beta^{-1} = a_1 a_2 \ldots a_n b_m^{-1} b_{m-1}^{-1} \ldots b_1^{-1}$ is a product of finite number of cycles.

Hence $\alpha\beta^{-1} \in H$ and so $H \leq G$.

PROBLEM 4.13 Show that for $n \geq 3$, $Z(S_n) = \{I\}$.

SOLUTION Let $f \in Z(S_n)$ be any member such that $f \neq I$.

Then there exist $a \neq b$ such that $f(a) = b$.

Let c be any other element such that $c \neq a$, $c \neq b$ and let $g \in S_n$ be the map in which $g(a) = a$, $g(b) = c$, $g(c) = b$.

Then $(fg)(a) = f(g(a)) = b$ and $(gf)(a) = g(f(a)) = c$.

Thus $fg \neq gf$ implying $f \notin Z(S_n)$, which is a contradiction.

Therefore, $f = I$ and hence $Z(S_n) = \{I\}$.

Problem 4.14 Let $\beta = (1\ 2\ 3)(1\ 4\ 5)$. Write β^{99} in cycle form.

Solution As $\beta = (1\ 2\ 3)(1\ 4\ 5) = (1\ 4\ 5\ 2\ 3)$. Therefore, $o(\beta) = 5$

Thus, $\beta^5 = I$ implying $\beta^{100} = I$.

Therefore, $\beta^{99} = \beta^{-1} = (3\ 2\ 5\ 4\ 1) = (1\ 3\ 2\ 5\ 4)$.

Problem 4.15 Let $\beta \in S_7$ and suppose $\beta^4 = (2\ 1\ 4\ 3\ 5\ 6\ 7)$. Find β.

Solution Since length of cycle β^4 is 7, we have $o(\beta^4) = 7$.

Now $\beta^8 = \beta^4 \cdot \beta^4 = (2\ 1\ 4\ 3\ 5\ 6\ 7)(2\ 1\ 4\ 3\ 5\ 6\ 7)$

$= (2\ 4\ 5\ 7\ 1\ 3\ 6)$

Thus, $\beta \cdot \beta^7 = (2\ 4\ 5\ 7\ 1\ 3\ 6)$.

Since $\beta \in S_7$, we have $\beta^7 = I$. Hence $\beta = (2\ 4\ 5\ 7\ 1\ 3\ 6)$.

4.5 Even and Odd Permutations

Definition 4.10: A permutation that can be written as a product of an even number of 2-cycles is called an **even permutation.**

Definition 4.11: A permutation that can be written as a product of an odd number of 2-cycles is called an **odd permutation.**

What we are asserting, therefore, is that every permutation is unambiguously either odd or even.

Problem 4.16 (a) If k is even, then prove that a k-cycle is odd.

(b) If k is odd, then prove that a k-cycle is even.

Solution Let $\sigma = (a_1 a_2 \ldots a_k)$ be any cycle of length k. Then

$$\sigma = (a_1 a_k)(a_1 a_{k-1}) \ldots (a_1 a_2)$$

is a product of $(k - 1)$ number of 2- cycles.

Now $k - 1$ is even or odd according as k is odd or even.

Thus, σ is a product of even (odd) number of transpositions according as k is odd (even).

Hence, σ is even permutation if k is odd and σ is odd permutation if k is even.

PROBLEM 4.17 Prove that inverse of every even (odd) permutation is even (odd).

SOLUTION Let $\alpha = (a_1b_1)(a_2b_2) \ldots (a_nb_n)$.

Then, $\alpha^{-1} = (a_nb_n)(a_{n-1}b_{n-1}) \ldots (a_1b_1)$

If α is even (odd), then α^{-1} is even (odd).

For example, let $\alpha = (1\ 2\ 3\ 4) = (14)(13)(12)$, then $\alpha^{-1} = (12)(13)(14)$.

THEOREM 4.5: Prove that:

(a) The product of two even permutations is also an even permutation.

(b) The product of two odd permutations is an even permutation.

(c) The product of an odd permutation and an even permutation is an odd permutation.

Proof:

(a) Let α and β be two even permutations. Then, both α and β are expressible as product of even number of transpositions.

Let $\alpha = \theta_1\theta_2 \ldots \theta_k$ and $\beta = \varphi_1\varphi_2 \ldots \varphi_l$, where l, k are even numbers and θ_i, φ_j are transpositions.

Then $\alpha\beta = \theta_1\theta_2 \ldots \theta_k\varphi_1\varphi_2 \ldots \varphi_l$.

Therefore $\alpha\beta$ is expressed as product of $l + k$ transpositions.

Thus $\alpha\beta$ is even permutation, as $l + k$ is an even number.

(b) Let α and β be odd permutations. Then, both are expressed as product of odd number of transpositions. Then, as above, we have $\alpha\beta$ is expressed as product of $l + k$ transpositions. Since in this case, both l, k are odd numbers, so $l + k$ is even. Therefore, $\alpha\beta$ is even permutation.

(c) Let α be odd and β be an even permutation, then, let

$\alpha = \theta_1\theta_2 \ldots \theta_k$ and $\beta = \varphi_1\varphi_2 \ldots \varphi_l$, where k is odd and l is even.

Then $l + k$ is odd and so, as discussed earlier, we see that $\alpha\beta$ is odd permutation.

Remark: Note that since $(1\ 2\ 3 \ldots (n-1)n) = (1n)(1n-1) \ldots (1\ 3)(1\ 2)$, is a product of $(n - 1)$ transpositions.

Also, if n is odd(even), then $(n - 1)$ is even(odd).

Therefore, a cycle of even(odd) length is an odd(even) permutation.

Problem 4.18 Prove that there is no permutation $a \in S_n$ such that

$$a^{-1}(12)a = (34)(15) \qquad \ldots(1)$$

Solution Clearly, right-hand side of (1) is an even permutation.

Let $a \in S_n$ be an even permutation.

Then, a^{-1} is an even permutation and (12) is an odd permutation.

Thus, $a^{-1}(12)$ is an odd permutation and therefore $a^{-1}(12)a$ is an odd permutation.

Now, let $a \in S_n$ be an odd permutation.

Then a^{-1} is an odd permutation and (12) is an odd permutation.

Hence $a^{-1}(12)$ is an even permutation and therefore $a^{-1}(12)a$ is an odd permutation.

Thus left hand side of (1) is always an odd permutation for each $a \in S_n$ and right hand side of (1) is an even permutation.

This is impossible and so the result follows.

Lemma 4.2: Let $I = \sigma_1\sigma_2 \ldots \sigma_k$, where $\sigma_i's$ are transpositions, then k is even.

Proof: Clearly $k \neq 1$ as if $I = (1)$, which can never be a 2-cycle.

Also, if $k = 2$, then I being product of two transpositions is even and we are done.

We proceed by induction on k.

Let the result be true for all $n < k$, i.e., whenever I is written as a product of say 'n' 2-cycles, where $n < k$, then n is even.

Now $I = \sigma_1\sigma_2 \ldots \sigma_k$. We need to show that k is even.

Consider $\sigma_1\sigma_2$: It will exactly be one of the following:

1. $(ab)(ab) = I$
2. $(ab)(bc) = (bc)(ac)$
3. $(ab)(ac) = (bc)(ab)$
4. $(ab)(cd) = (cd)(ab)$

In case (1), $I = \sigma_3\sigma_4 \ldots \sigma_k$, i.e., product of $(k - 2)$ 2-cycles.

Therefore, by induction hypothesis (since $k - 2 < k$), we get $k - 2$ is even, hence k is even.

In cases (2), (3) and (4), observe that 'a' has been shifted to the second 2-cycle, i.e., first occurrence of the element 'a' is in the second cycle.

Let us proceed the same way now for $(ac)\sigma_3$. Either $(ac)\,\sigma_3 = I$ in which case $I = \sigma_1\,\sigma_4 \ldots \sigma_k$ and again by induction hypothesis $(k - 2)$ is even and so is k or else I can be written as a product of k-cycles where 'a' gets shifted to third cycle.

Proceeding like this, we must get I as a product of $(k-2)$ 2-cycles, because otherwise I will be a product of k 2-cylces where 'a' occurs first time in the last 2-cycle but then 'a' is not fixed (i.e., 'a' is not mapped to 'a') whereas I fixes 'a'.

So, I can definitely be written as a product of $(k-2)$ 2-cycles and by induction hypothesis, $(k-2)$ is even and so k is even.

THEOREM 4.6: If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even(odd) number of 2-cycles.

In symbols, if $\alpha = \sigma_1\sigma_2 \ldots \sigma_r$ and $\alpha = \tau_1\tau_2 \ldots \tau_s$, where σ_i' *s* and τ_i' *s* are 2-cycles, then r and s are both even or both odd.

Proof:

We have, $\sigma_1\sigma_2 \ldots \sigma_r = \tau_1\tau_2 \ldots \tau_s$.

Then $I = \tau_1\tau_2 \ldots \tau_s\sigma_r^{-1} \ldots \sigma_2^{-1}\sigma_1^{-1} = \tau_1\tau_2 \ldots \tau_s\sigma_r \ldots \sigma_2\sigma_1$.

(Since the inverse of a transposition is itself).

Also by Lemma 4.2, $r + s$ is even, we have either r and s are both even or both odd.

THEOREM 4.7: If H is a subgroup of S_n, then either every member of H is an even permutation or exactly half of them are even.

Proof: If every member of H is an even permutation, then we are done.

Let A be the set of all even permutations in H and B be the set of all odd permutations in H.

Let σ be an odd permutation in H.

As we know that product of an even permutation and an odd permutation is odd permutation. Therefore, $\sigma A \subseteq B$.

Hence, $o(\sigma A) \leq o(B)$. Also, $o(\sigma A) = o(A)$.

Therefore, $o(A) \leq o(B)$ ...(1)

Again, as product of two odd permutations is an even permutation. Therefore $\sigma B \subseteq A$ implying $o(\sigma B) \leq o(A)$.

Also $o(\sigma B) = o(B)$. Hence, $o(B) \leq o(A)$ ...(2)

From (1) and (2), we get $o(A) = o(B)$.

And so, in this case, exactly half are odd and half are even permutations in H.

PROBLEM 4.19 How many odd permutations of order 4 does S_6 have?

SOLUTION An odd permutation of order 4 must be of the form $(a_1a_2a_3a_4)$.

There are 6 choices for a_1, 5 choices for a_2, 4 choices for a_3, 3 for a_4.

Thus there are 6·5·4·3 choices.

But for each of these choices, the cycles $(a_1a_2a_3a_4) = (a_2a_3a_4a_1) = (a_3a_4a_1a_2) = (a_4a_1a_2a_3)$ give the same group element.

Thus number of odd permutations of order 4 = 6·5·4·3/4 = 90 permutations.

Problem 4.20 Let α and β belong to S_n. Prove that $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation.

Solution The following different cases may arise for α and β:

(a) When both α and β are even.

Then, α^{-1} and β^{-1} are both even. Therefore, $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.

(b) When both α and β are odd

Then, α^{-1} and β^{-1} are both odd and hence, $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.

(c) Let α be odd and β be even

Then, α^{-1} is odd and β^{-1} is even and thus, $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.

(d) Let α be even and β be odd

Then, α^{-1} is even and β^{-1} is odd. Therefore, $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.

Theorem 4.8: The set of even permutations in S_n forms a subgroup of S_n.

Proof: Let K be the set of all even permutations in S_n.

Clearly, $K \neq \varphi$, since I is an even permutation and so $I \in K$.

Let $f, g \in K$.

Let f be a product of $2k$ 2-cycles and g be a product of $2p$ 2-cycles,

i.e., $f = \alpha_1\alpha_2 \ldots \alpha_{2k}$ and $g = \beta_1\beta_2 \ldots \beta_{2p}$

Then $f \circ g = fg = (\alpha_1\alpha_2 \ldots \alpha_{2k})(\beta_1\beta_2 \ldots \beta_{2p})$ is a product of $2k + 2p = 2(k + p)$ 2-cycles.

So, $f \circ g \in K, \forall f, g \in K$

Since K is finite, being a subset of S_n, so by finite subgroup test, K is a subgroup of S_n.

4.6 Alternating Group of Degree *n*

The subgroup of even permutations in S_n arises so often that we give it a special name and notation.

Definition 4.12: The group of even permutations of S_n is called the **alternating group of degree *n*** and is denoted by A_n.

For example, the set of even permutations in S_4 is:

$$A_4 = \left\{ \begin{matrix} (123), (132), (124), (142), (134), (143), (234), \\ (243), (12)(34), (13)(24), (14)(23), (1) \end{matrix} \right\}$$

PROBLEM 4.21 How many elements of order 5 are there in A_6?

SOLUTION

An element of order 5 in A_6 must be a 5 - cycle.

And there are $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 720$ ways to create a 5-cycle.

But same 5-cycle can be written in 5 ways.

Therefore, there are $720/5 = 144$ elements of order 5 in A_6.

The next theorem shows that exactly half of the elements of $S_n (n > 1)$ are even permutations.

THEOREM 4.9: For $n > 1$, A_n has order $\frac{n!}{2} = \frac{o(S_n)}{2}$.

Proof: We have, $o(S_n) = n!$.

Out of $n!$ permutations, let $e_1, e_2, ..., e_m$ be even permutations and $\sigma_1, \sigma_2, ..., \sigma_k$ be odd permutations.

Since a permutation is either even or odd but not both, thus,

$$m + k = n! \qquad ...(1)$$

And $$S_n = \{e_1, e_2, ..., e_m, \sigma_1, \sigma_2, ..., \sigma_k\}.$$

Let $t \in S_n$ be such that t is an odd permutation.

Since S_n is a group, therefore $te_1, te_2, ..., te_m, t\sigma_1, t\sigma_2, ..., t\sigma_k$ are all members of S_n.

Clearly, $te_i's$ are odd permutations for $i = 1$ to m and $t\sigma_j's$ are even permutations for $j = 1$ to k.

Also, all are distinct since if $te_i = te_j$ for some $i \neq j$, then $e_i = e_j$, a contradiction.

Also, since we have assumed that S_n has exactly k odd permutations, therefore $m \leq k$.

Similarly, we have exactly m even permutations therefore, $k \leq m$.

$\therefore\ k = m$ and thus by (1), we have $m + k = 2m = n!$.

Therefore, $m = \frac{n!}{2}$, which gives $o(A_n) = \frac{o(S_n)}{2} = \frac{n!}{2}$.

PROBLEM 4.22 Using the fact that order of elements of A_4 is 1, 2 or 3, prove that $|Z(A_4)| = 1$.

SOLUTION

We have, $Z(G) = \{z \in G : zg = gz, \forall\ g \in G\}$

Then, $$Z(A_4) = \{z \in A_4 : zg = gz, \forall\ g \in A_4\}$$

Since $I \in Z(A_4)$, we have $Z(A_4) \neq \phi$.

Let $a \in Z(A_4)$ be any element of order 2 and let $b \in A_4$ be such that $o(b) = 3$.

Then gcd(o(a), o(b)) = 1 and since $a \in Z(A_4)$ and $b \in A_4$, therefore we have, $ab = ba$.

Thus, $o(ab) = o(a)\ o(b) = 2.3 = 6$, which is not true as $ab \in A_4$ and order of elements of A_4 is 1, 2 or 3.

Hence $Z(A_4)$ does not contain any element of order 2.

Now let $a \in Z(A_4)$ be any element of order 3 and let $b \in A_4$ be of order 2.

Then as discussed above, $o(ab) = 6$, which is not true.

Hence $Z(A_4)$ does not contain any element of order 3.

Thus $Z(A_4)$ contains only elements of order 1, i.e., identity permutation.

Therefore $|Z(A_4)| = 1$.

PROBLEM 4.23 Show that every element in A_n, for $n \geq 3$, can be expressed as a 3-cycle or a product of 3-cycles.

SOLUTION Let $\alpha \in A_n$ be any element.

Then, α can be expressed as a product of even number of transpositions.

Let $\alpha = \alpha_1\alpha_2\alpha_3\alpha_4 \ldots \alpha_{2k-1}\ \alpha_{2k} = (\alpha_1\alpha_2)(\alpha_3\alpha_4) \ldots (\alpha_{2k-1}\alpha_{2k})$.

Now each pair $\alpha_j\ \alpha_{j+1}$ can be any one of the forms

$$(ab)(ab),\ (ab)(bc) \text{ or } (ab)(cd)$$

We consider them one by one.

Case I: we have $(ab)(ab) = I = (abc)(cba)$, product of 3–cycles.

Case II: $(ab)(bc) = (acb)$, is a 3-cycle.

Case III: $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$, product of 3–cycles.

Thus, each pair $\alpha_j\ \alpha_{j+1}$ is either a 3-cycle or expressed as product of 3–cycles.

Hence, α is a product of 3-cycles.

EXERCISES

1. Find an element of order 15 in A_8.
2. In A_{10}, find an element of maximum order.
3. How many elements of order 5 are in S_7?
4. Determine whether the following permutations are even or odd.
   (a) (135)
   (b) (1356)
   (c) (13567)
   (d) (1 2 4 3)(3 5 2 1)

5. Prove that (1 2 3 4) is not the product of 3-cycles.

6. Do the odd permutations in S_n form a group? Why?

7. In S_5, find elements α and β so that $o(\alpha) = 3$, $o(\beta) = 3$ and $o(\alpha\beta) = 5$.

8. Find the order of all the elements of S_3.

9. Let α = (23415)(4768) and β = (4397)(8)(15274). Write $\alpha\beta$ and $\beta\alpha$ as product of disjoint cycles. Is $\alpha\beta = \beta\alpha$?

10. Prove that α = (3 6 7 9 12 14) $\in S_{16}$ is not a product of 3-cycles.

11. Find two elements, say, a and b, in a group such that $o(a) = o(b) = 2$, and $o(ab) = 3$.

12. Give an example of two elements, say, a and b, such that $o(a) = 2$, $o(b) = 3$ and $o(ab) \neq \text{lcm}(2, 3) = 6$.

13. Let $H = \{\alpha \in S_n : \alpha(1) = 1\}$ $(n > 1)$. Prove that H is a subgroup of S_n.

14. Let $n > 1$. Prove that S_n contains a subgroup of order $(n - 1)!$.

15. Express the following permutations as products of disjoint cycles:

(i) (1 2 3)(4 5)(1 3 4 5)

(ii) (1 2)(5 4)(3 2)(1 7)(2 8)

(iii) (4 5)(1 2 3)(3 2 1)(5 4)(2 6)(1 4).

HINTS TO SELECTED PROBLEMS

1. σ = (1 2 3)(4 5 6 7 8) $\in A_8$

2. σ = (1 2 3)(4 5 6 7 8 9 10) $\in A_{10}$ with $o(\sigma) = 21$.

3. $$\frac{7!}{5.(7-5)!} = \frac{7\times 6\times 5\times 4\times 3}{5} = 504$$

10. Since α = (3 14)(3 12) ... (3 6) is a product of five 2-cycles, α is an odd cycle. Since each 3-cycle is an even cycle. Thus, α is never a product of 3-cycles.

11. Consider the group S_3. Let a = (1 2), b = (1 3). Then, ab = (1 2)(1 3) = (1 3 2). Hence, $o(a) = o(b) = 2$, and $o(ab) = 3$.

12. Let $G = S_3$. Let a = (1 2), b = (1 2 3). Then, ab = (2 3). Hence, $o(a) = 2$, $o(b) = 3$, and $o(ab) = 2 \neq \text{lcm}(2, 3) = 6$.

13. Let α and $\beta \in H$. Since $\alpha(1) = 1$ and $\beta(1) = 1$, $\alpha\beta(1) = \alpha(\beta(1)) = 1$. Hence, $\alpha\beta \in H$. Since H is a finite set (being a subset of S_n) and closed, H is a subgroup of S_n.

14. Let H be the subgroup of S_n described in the previous question. It is clear that $o(H) = (n - 1)!$.

❑❑❑

Check for updates

5

Cosets and Lagrange's Theorem

Learning Objectives

- Definition and Properties of Cosets
- Lagrange's Theorem and its Applications
- Application of Cosets to Permutation Groups

5.1 Definition of Cosets and Properties of Cosets

Let us define Cosets and discuss properties of Cosets. Cosets are crucial to the study of groups, as they help in understanding a factor group as well as the Lagrange's† Theorem, a seminal theorem in group theory, which, incidentally, may also be used to derive Euler's stheorem, a foundational result in number theory. As these fundamental results were discovered separately in the two fields, independent of mutual influence or intervention, they suggest profound resonances between group theory and number theory.

Cosets have instrumental applications in computer science, for example, in the development of efficient codes needed for the transmission of information.

Definition 5.1: Let G be a group and H be a subset of G. Let $a \in G$.

Define $Ha = \{ha : h \in H\}$ and $aH = \{ah : h \in H\}$

If H is a subgroup of G, then the set aH is called the **left coset of H in G** and the set Ha is called the **right coset of H in G.**

The element 'a' is called the **coset representative of aH (or Ha).**

We use $|aH|$ to denote the number of elements in the set aH and $|Ha|$ to denote the number of elements in Ha.

† Joseph-Louis Lagrange, an Italian-born French mathematician who made significant contributions in all fields of analysis and number theory and analytical and celestial mechanics.

© The Author(s) 2023

D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_5

Note that if G is an additive group, then the left coset aH is written as $a + H$ and is defined as

$$a + H = \{a + h : h \in H\}.$$

The right coset can also be defined in the similar manner.

Example 5.1: Let $G = \mathbb{Z}$, the group of integers under addition and let

$$H = 2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}.$$

Then, the right cosets of H in G are given by

$$H + 0 = \{2m + 0 : m \in \mathbb{Z}\} = \{2m : m \in \mathbb{Z}\} = H.$$

$$H + 1 = \{2m + 1 : m \in \mathbb{Z}\} = \{... -5, -3, -1, 1, 3, 5, ...\}$$

$$H + 2 = \{2m + 2 : m \in \mathbb{Z}\} = \{... -4, -2, 0, 2, 4, ...\} = H.$$

$$H + 3 = \{2m + 3 : m \in \mathbb{Z}\} = \{... -5, -3, -1, 1, 3, 5, 7, 9 ...\} = H + 1.$$

$$H + (-1) = \{2m + (-1) : m \in \mathbb{Z}\} = \{... -5, -3, -1, 1, 3, 5,...\} = H + 1.$$

and so on.

We observe that there are only two right cosets of H in G, namely H and $H + 1$.

The left cosets can also be found using the same discussion.

Example 5.2: Let $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$ and $H = \{(1), (23)\}$. Then, all the left cosets of H in G are:

$$(1)H = \{(1), (23)\} = H,$$

$$(12)H = \{(12)(1), (12)(23)\} = \{(12), (123)\},$$

$$(13)H = \{(13)(1), (13)(23)\} = \{(13), (132)\},$$

$$(23)H = \{(23)(1),(23)(23)\} = \{(23), (1)\},$$

$$(123)H = \{(123)(1), (123)(23)\} = \{(123), (12)\},$$

and $$(132)H = \{(132)(1), (132)(23)\} = \{(132), (13)\}.$$

Similarly, we can find all the right cosets as

$$H(1) = \{(1), (23)\} = H,$$

$$H(12) = \{(1)(12), (23)(12)\} = \{(12), (132)\},$$

$$H(13) = \{(1)(13), (23)(13)\ \} = \{(13), (123)\},$$

$$H(23) = \{(1)(23),(23)(23)\} = \{(23), (1)\},$$

and $$H(123) = \{(1)(123), (23)(123)\} = \{(123), (13)\},$$

$$H(132) = \{(1)(132), (23)(132)\} = \{(132), (12)\}.$$

Example 5.3: Let $H = \{0, 3, 6\}$ in $\mathbb{Z}_9$, the group of integers under addition modulo 9.

We have, $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

The left cosets of H in G are as follows

$$0 + H = \{0, 3, 6\} = 3 + H = 6 + H,$$
$$1 + H = \{1, 4, 7\} = 4 + H = 7 + H,$$
$$2 + H = \{2, 5, 8\} = 5 + H = 8 + H.$$

Example 5.4: Let $G = D_4$ and let $K = \{R_0, R_{180}\}$.

Then, the right cosets of K in G are:

$$KR_0 = \{R_0, R_{180}\} = KR_{180} = K,$$
$$KR_{90} = \{R_{90}, R_{270}\} = KR_{270},$$
$$KF_H = \{F_H, F_V\} = KF_V$$

and
$$KF_D = \{F_D, F_{D'}\} = KF_{D'}$$

Example 5.5: Let $G = \mathbb{Z}$, the group of integers under addition and let $K = \{0\}$.

Then, the right cosets of K in G are of the form

$K + a = \{k + a : a \in G\} = \{a\}$, for all a in G.

Hence, there are infinitely many right cosets of K in G.

The above examples show that cosets are usually not subgroups.

Also, aH may be the same as bH, even though a is not the same as b. Finally, aH need not be the same as Ha.

So, we have the following questions.

1. When does $aH = bH$?
2. When does $aH = Ha$?
3. Which cosets are subgroups?

To answer these questions, we have the following Lemma.

Lemma 5.1: Let H be a subgroup of a group G and let a and b belong to G. Then,

1. $a \in aH$
2. $aH = H$ if and only if $a \in H$
3. Any two left cosets of H in G are either identical or disjoint. That is either $aH = bH$ or $aH \cap bH = \phi$
4. $aH = bH$ if and only if $a^{-1}b \in H$
5. $|aH| = |bH|$, i.e., any two left cosets of H in G have the same order
6. $aH = Ha$ if and only if $H = aHa^{-1}$.
7. aH is a subgroup of G if and only if $a \in H$.

Proof:

1. Since $a = ae \in aH$, we have that $a \in aH$.
2. Let $a \in H$. To show: $aH = H$.

   Let $h \in H$. Since $a, h \in H$ and H is a subgroup of G, we get $a^{-1}h \in H$

   Thus, $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$, implying $H \subseteq aH$.

   Now, let $x \in aH$, then $x = ah$ for some $h \in H$.

   Since $a \in H$ and $h \in H$, we have $x \in H$.

   Thus, $aH \subseteq H$. Therefore, $aH = H$.

   Conversely, let $aH = H$. Then, $a = ae \in aH = H$ implying that $a \in H$.
3. If $aH \cap bH = \phi$, then there is nothing to prove.

   Suppose $aH \cap bH \neq \phi$. We will prove that $aH = bH$.

   Let $x \in aH \cap bH$. Then, $x \in aH$ and $x \in bH$.

   So there exist h_1, h_2 in H such that $x = ah_1$ and $x = bh_2$.

   This gives $a = xh_1^{-1} = bh_2h_1^{-1}$ and $aH = bh_2h_1^{-1}H = bH$

   (since $h_2h_1^{-1} \in H$, followed by property 2)

   Therefore, $aH = bH$.

   Remark: The above result can be restated as:
   Two distinct left(right) cosets of H in G must be disjoint.

4. We have, $aH = bH$

   $\Leftrightarrow$ $a^{-1}(aH) = a^{-1}(bH)$

   $\Leftrightarrow$ $(a^{-1}a)H = (a^{-1}b)H$

   $\Leftrightarrow$ $eH = a^{-1}bH$

   $\Leftrightarrow$ $H = a^{-1}bH$

   $\Leftrightarrow$ $a^{-1}b \in H$ (Using Property 2)

   Note that for right cosets, $Ha = Hb \Leftrightarrow ab^{-1} \in H$ or $ba^{-1} \in H$.
5. **Case I:** If H is finite, we will prove that $o(aH) = o(H)$.

   Let $H = \{h_1, h_2, \ldots, h_n\}$. Then, $aH = \{ah_1, ah_2, \ldots ah_n\}$

   We assert that $ah_1, ah_2, \ldots, ah_n$ are all distinct.

   If possible, suppose $ah_i = ah_j$ for some $i \neq j$.

   Then, $h_i = h_j$, by left cancellation law. This gives a contradiction.

   Thus, all $ah_1, ah_2, \ldots, ah_n$ are distinct and therefore $o(aH) = o(H)$.

   Similarly, $o(bH) = o(H)$.

   Thus, in this case, $|aH| = |bH|$.

Case II: If H is infinite, we assert that the correspondence $aH \to bH$ is one-one and onto.

Define $\varphi : aH \to bH$ by $\varphi(aH) = bH, \forall h \in H$

Let $ah_1 = ah_2$ then $h_1 = h_2$ (by left cancellation law)

This implies $bh_1 = bh_2$ and hence, $\varphi(ah_1) = \varphi(ah_2)$.

Thus, φ is well defined.

To show φ is one-one, let $\varphi(ah_1) = \varphi(ah_2)$

$\Rightarrow$ $bh_1 = bh_2$

$\Rightarrow$ $h_1 = h_2$ (by left cancellation law)

$\Rightarrow$ $ah_1 = ah_2$

Hence, φ is one-one.

Clearly, φ is onto, as for every $bh \in bH$, there exists some $ah \in aH$ such that $\varphi(ah) = bh$.

Hence, φ is a bijection and therefore $|aH| = |bH|$.

6. We have,

$$aH = Ha \Leftrightarrow (aH)a^{-1} = (Ha)a^{-1} \Leftrightarrow aHa^{-1} = H.$$

7. Let aH be a subgroup of G, then $e \in aH$

$\Rightarrow$ $e = ah$ for some $h \in H$

$\Rightarrow$ $eh^{-1} = ahh^{-1} = ae = a$

$\Rightarrow$ $h^{-1} = a$

$\therefore$ $a = h^{-1} \in H$ (As H is a subgroup of G)

Conversely, let $a \in H$. Then, by property 2, we have $aH = H$.

Since H is a subgroup of G, therefore aH is a subgroup of G.

PROBLEM 5.1 Let $H = \{0, \pm3, \pm6, \pm9, ...\}$.
Decide whether or not the following cosets of H are the same.
(a) $11 + H$ and $17 + H$
(b) $-1 + H$ and $5 + H$
(c) $7 + H$ and $23 + H$

SOLUTION

(a) We have $17 + H = 11 + (6 + H) = 11 + H$ (as $6 \in H$, so $6 + H = H$).
Therefore, $11 + H = 17 + H$

(b) We have $-1 + H = -1 + (6 + H) = 5 + H$. Thus, $-1 + H = 5 + H$.

(c) We can write $23 + H = 5 + (18 + H) = 5 + H$ (as $18 \in H$, so $18 + H = H$).
Therefore $23 + H \neq 7 + H$.

Problem 5.2 Let $H = \{0, \pm 3, \pm 6, \pm 9, ...\} = 3\mathbb{Z}$. Find all the left cosets of H in $\mathbb{Z}$.

Solution We have, H is a subgroup of $\mathbb{Z}$.

Then the left cosets of H in $\mathbb{Z}$ are H, $1 + H$, $2 + H$.

We show that there are no other left cosets.

For any integer n, we can write $n = 3q + r$, where $0 \leq r < 3$.

So, $n + H = r + 3q + H = r + H$ ($\because$ $3q \in H$, so $3q + H = H$)

where $r = 0$, 1 or 2. So, there are no other left cosets.

Problem 5.3 Let n be an integer greater than 1. Let $H = \{0, \pm n, \pm 2n, ...\}$. Find all left cosets of H in $\mathbb{Z}$. How many are there?

Solution We have, $H = \{0, \pm n, \pm 2n, \pm 3n, ...\} = \langle n \rangle$.

Then, the left cosets of H in $\mathbb{Z}$ are

$0 + \langle n \rangle$, $1 + \langle n \rangle$, $2 + \langle n \rangle$, $3 + \langle n \rangle$, ..., $(n - 1) + \langle n \rangle$, $n + \langle n \rangle$, $(n + 1) + \langle n \rangle$ and so on.

Now, $n + \langle n \rangle = \langle n \rangle$ ($\because$ $n \in H$, $\therefore$ $n + \langle n \rangle = \langle n \rangle$)

and $(n + 1) + \langle n \rangle = 1 + (\langle n \rangle + n) = 1 + \langle n \rangle$.

Thus, the only left cosets are

$$0 + \langle n \rangle = \langle n \rangle, 1 + \langle n \rangle, 2 + \langle n \rangle, 3 + \langle n \rangle, ... (n - 1) + \langle n \rangle$$

To prove: there are no other left cosets.

For any integer k, we write $k = nq + r$, $0 \leq r < n$.

Then, $k + H = k + \langle n \rangle = nq + r + \langle n \rangle = nq + \langle n \rangle + r = r + \langle n \rangle$

where, $r = 0, 1, 2, ..., n - 1$.

Thus, there are no other left cosets.

5.2 Lagrange's Theorem and its Applications

In our study of subgroups, we noticed that in a finite group, the order of each of its subgroups was a divisor of the order of the group. This is a very important result of the finite groups, known as the Lagrange's Theorem, having interesting implications in number theory. This theorem gives us the possible orders of the subgroups of a finite group. One important use of theorem is that it significantly narrows down the possibilities for subgroups. For example, in a group of order 6, we know not to bother looking for subgroups of order 4 or 5 as these numbers do not divide 6.

Theorem 5.1: If G is a finite group and H is a subgroup of G, then $o(H)$ divides $o(G)$, i.e., the order of any subgroup of a finite group is a divisor of the order of the group.

Proof: Let H be a subgroup of a finite group G and let $\{aH : a \in G\}$ be the set of all left cosets of H in G.

Since G is a finite group, the number of left cosets of H in G is finite.

Further, some of the left cosets may be identical, so we have to choose only the distinct ones.

Let $S = \{a_1H, a_2H, \ldots, a_mH\}$ denote the distinct left cosets of H in G.

We show that the union of these cosets is G.

Let $a \in G$. Then, $a \in aH$ and also $aH = a_iH$ for some i. Thus, $a \in a_iH$.

$\Rightarrow \quad a \in a_1H \cup a_2H \ldots \cup a_mH$

$\Rightarrow \quad G \subseteq a_1H \cup a_2H \ldots \cup a_mH$

$\Rightarrow \quad G = a_1H \cup a_2H \ldots \cup a_mH$

Since the distinct left cosets are disjoint, we have

$$o(G) = o(a_1H) + o(a_2H) + \ldots + o(a_mH)$$

Therefore $\quad o(G) = o(H) + o(H) + \ldots + o(H) \qquad (m \text{ times})$

Thus $o(G) = m\, o(H)$ and hence $o(H) | o(G)$.

Corollary 5.1: The number of distinct left (right) cosets of H in G is $\dfrac{o(G)}{o(H)}$.

Proof: From the Theorem, we have, $\dfrac{o(G)}{o(H)} = m =$ number of distinct left (right) cosets of H in G.

Definition 5.2: Let G be a group and H be a subgroup of G. The **index of H in G**, denoted by $|G : H|$ or $i_G(H)$, is the number of distinct left(right) cosets of H in G.

Note that the converse of Lagrange's theorem in general is not true. That is, if G is a finite group of order n, then it need not be true that for every divisor k of n there is a subgroup of G of order k.

Example 5.6: Consider the alternating group A_4.

Then $\quad o(A_4) = \dfrac{o(S_4)}{2} = \dfrac{4!}{2} = 12.$

Thus A_4 is a group having 12 elements.

Now $6 | 12 = o(A_4)$, but we will show that A_4 has no subgroup of order 6.

Let, if possible, H be a subgroup of A_4 such that $o(H) = 6$.

Also $\quad i_G(H) = \dfrac{12}{6} = 2.$

Thus H has exactly 2 distinct left cosets in G.

Now A_4 has 8 elements of order 3.

Let a be any element of A_4 with order 3. Then, $a^3 = e$.

Consider the left cosets H, aH, a^2H.

Since there are only two distinct left cosets, so any two of them must be equal.

Case I: If $H = aH$, then $a \in H$

Case II: If $H = a^2H$, then $aH = a^3H = H$ implying $a \in H$.

Case III: If $aH = a^2H$, then $a^{-1}a^2 \in H$, so $a \in H$.

Therefore, in either case, $a \in H$.

Since a was any arbitrary element of A_4 with order 3, we get that H contains all elements of order 3. But $o(H) = 6$ and there are 8 elements of order 3.

This gives a contradiction and hence, A_4 has no subgroup of order 6.

The question which now arises in our mind is:

Will the converse of Lagrange's Theorem hold in certain cases?

The answer is yes. It does hold for a finite cyclic group.

So, we have the following theorem.

Theorem 5.2: Converse of Lagrange's Theorem holds in a finite cyclic group, i.e., if G is a finite cyclic group of order n, then for every divisor m of n, there is a subgroup of G of order m.

Proof: Let $G = \langle a \rangle$ be a finite cyclic group and let $o(G) = o(a) = n$.

Suppose $m|n$.

We will show that G has a subgroup of order m.

Since $m|n$, there exists some $k \in \mathbb{Z}$ such that $n = km$.

Consider the element a^k and let $H = \langle a^k \rangle$. Then, H is a subgroup of G.

We show that $o(H) = o(\langle a^k \rangle) = m$.

Now, $(a^k)^m = a^{km} = a^n = e$.

Let $(a^k)^r = e$, then $a^{kr} = e$. This gives $n|kr$.

Then, $km|kr$ and so $m|r$. Thus, $m \leq r$.

Therefore, G has a subgroup of order m.

There are some useful Corollaries due to Lagrange's Theorem.

Corollary 5.2: In a finite group, the order of each element of the group divides the order of the group.

Proof: Let G be a finite group and $a \in G$. Let $H = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

Then, H is a subgroup of G.

Since $H = \langle a \rangle$ is cyclic, $o(H) = o(a)$.

By Lagrange's theorem, we have $o(H)|o(G)$. Thus, $o(a)|o(G)$.

Corollary 5.3: A group of prime order is cyclic.

Proof: Let G be a group such that $o(G) = p$, where p is prime.

Then, there exists $a \in G$ such that $a \neq e$.

By Corollary 5.2, $o(a) \mid o(G)$.

Also, since $\langle a \rangle$ is a subgroup of G, by Lagrange's theorem, we have

$$o(\langle a \rangle) \mid o(G) = p$$

Thus, $o(\langle a \rangle) = 1$ or $o(\langle a \rangle) = p$. But $o(\langle a \rangle) \neq 1$ as $a \neq e$.

Therefore, $o(\langle a \rangle) = p$. Hence, $o(\langle a \rangle) = p = o(G)$.

Therefore, $G = \langle a \rangle$ and so, G is cyclic.

Corollary 5.4: Let G be a finite group and $a \in G$. Then, $a^{o(G)} = e$.

Proof: By Corollary 5.2, $o(a) \mid o(G)$.

Then, there exists some positive integer m such that $o(G) = m\, o(a)$.

Thus, $$a^{o(G)} = a^{mo(a)} = (a^{o(a)})^m = e^m = e.$$

When we apply the above result to certain special groups arising in number theory, we shall obtain some classical number-theoretic results due to Fermat and Euler†.

An important application of Lagrange's theorem is the Fermat's Little Theorem, given in the following Corollary.

Corollary 5.5: For every integer a and every prime p,

$$a^p \equiv a \text{ modulo } p.$$

Proof: By division algorithm,

$$a = pm + r, \text{ where } 0 \leq r < p.$$

i.e., $a = r \bmod p$ i.e., $a \equiv r$

i.e., it suffices to show $r^p \equiv r \bmod p$.

Now, if $r = 0$, the result is trivially true. So let $r \in \{1, 2, ..., p - 1\}$

Note that $\{1, 2, ..., p - 1\} = U(p)$, which is a group under multiplication modulo p.

By Corollary 5.4, $r^{p-1} = e$. Thus, $r^p \equiv r \bmod p$.

Hence the result.

---

† **Pierre de Fermat**, a French mathematician, mostly remembered for his work on theory of numbers; in particular for Fermat's Last Theorem.
Leonhard Euler, a Swiss mathematician and physicist and one of the giants of 18th Century mathematics, who made enormous contributions in various branches of pure mathematics such as analytic number theory, complex analysis, and infinitesimal calculus.

Problem 5.4 Let G be a group of order 60. What are the possible orders for the subgroup of G?

Solution Let $o(G) = 60$ and let H be a subgroup of G.

Then by Lagrange's Theorem, $o(H)$ divides $o(G)$.

Therefore $o(H) = 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ or 60.

Problem 5.5 Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $o(K) = 42$ and $o(G) = 420$, what are the possible orders of H?

Solution We have, K is a proper subgroup of H and H is a proper subgroup of G. Also, $o(K) = 42$ and $o(G) = 420$.

Therefore by Lagrange's Theorem, $o(H)$ is a multiple of $o(K)$.

Thus possible orders of H are 84, 126, 168, 210, 252, 294, 336, 378, 420

Also H is a subgroup of G, therefore $o(H)$ divides $o(G)$.

Now $o(H) \neq 420$, as H is a proper subgroup of G.

Also $o(H) \neq 126, 168, 252, 294, 336, 378$, as these are not divisors of $o(G)$.

Thus $o(H) = 84$ or 210.

Problem 5.6 Prove that the order of $U(n)$ is even, when $n > 2$.

Solution We already know that $(n - 1) \in U(n)$. Also, $o(n - 1) = 2$

(since $(n - 1)^2 = (n - 1)(n - 1) = n^2 + 1 - 2n = n(n - 2) + 1 \equiv 1$)

Since $o(n - 1) | o(U(n))$, therefore $o(U(n))$ is even.

Problem 5.7 Find all the left cosets of $\{1, 11\}$ in $U(30)$.

Solution $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$, under multiplication modulo 30 and $H = \{1, 11\}$,

Then $U(30)$ is a finite group and H is its subgroup.

By Lagrange's Theorem number of distinct left cosets of H in $U(30)$ is given by $\dfrac{o(U(30))}{o(H)} = \dfrac{8}{2} = 4$.

And these left cosets are

$$1H = \{1, 11\},\ 7H = \{7, 17\},\ 11H = \{11, 1\} = 1H,$$

$$13H = \{13, 23\},\ 17H = \{17, 7\} = 7H,\ 19H = \{19, 29\},$$

$$23H = \{23, 13\} = 13H,\ 29H = \{29, 19\} = 19H.$$

Thus the distinct left cosets are H, $13H$, $17H$ and $19H$.

Problem 5.8 Let $K = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of K in A_4.

Solution We have $K = \{(1), (12)(34), (13)(24), (14)(23)\}$.

A_4 is an alternating group consisting of all even permutations on the set $S = \{1, 2, 3, 4\}$.

Then,

$A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (243), (142), (134), (132), (143), (234), (124)\}$

The left cosets are defined as $aK = \{ak | k \in K\}$, for $a \in A_4$.

$$(1)K = \{(1), (12)(34), (13)(24), (14)(23)\} = K,$$
$$(12)(34)K = \{(12)(34), (1), (14)(23), (13)(24)\} = K,$$
$$(13)(24)K = \{(13)(24), (14)(23), (1), (12)(34)\} = K,$$
$$(14)(23)K = \{(14)(23), (13)(24), (12)(34), (1)\} = K$$
$$(123)K = \{(123), (134), (243), (142)\} = (132)K$$
$$(243)K = \{(243), (142), (123), (134)\} = (123)K$$
$$(142)K = \{(142), (243), (134), (123)\} = (123)K$$
$$(134)K = \{(134), (123), (142), (243)\} = (123)K$$
$$(132)K = \{(132), (234), (124), (143)\} = (132)K$$
$$(143)K = \{(143), (124), (234), (132)\} = (132)K$$
$$(234)K = \{(234), (132), (143), (124)\} = (132)K$$
$$(124)K = \{(124), (143), (132), (234)\} = (132)K$$

Therefore, the only left cosets of K in A_4 are K, $(123)K$ and $(132)K$.

Problem 5.9 Let K be as defined in the above problem. How many left cosets of K in S_4 are there?

Solution Number of elements in $S_4 = 4! = 24$ and number of elements in $K = 4$.

We know that S_4 is a finite group and K is a subgroup of S_4.

Therefore, by Lagrange's theorem, number of distinct left cosets of K in S_4 are $\frac{o(S_4)}{o(K)} = \frac{24}{4} = 6$.

Problem 5.10 Let G be a group. Prove or disprove that $H = \{g^2 : g \in G\}$ is a subgroup of G.

Solution We show that H may not be a subgroup of G.

Let $G = A_4$. Then, $o(A_4) = \frac{o(S_4)}{2} = \frac{24}{2} = 12$.

We have, $G = \{I,\ (12)(34),\ (13)(24),\ (14)(23),\ (123),\ (132),\ (243),\ (234),\ (124),\ (142),\ (143),\ (134)\}$

Take, $H = \{I, (123), (132), (243), (234), (124), (142), (143), (134)\}$

(Since $(123)^2 = (132)$, $(132)^2 = (123)$ and so on.)

Clearly, H is not a subgroup of $G = A_4$ as $9 \nmid 12$. (by Lagrange's Theorem)

Note: We have, $H = \{g^2 : g \in G\}$. Since $e = e \cdot e = e^2 \in H$. So, $H \neq \phi$.

Let $x, y \in H$ then $x = a^2$ and $y = b^2$, where $a, b \in G$.

Then $xy = a^2b^2 \neq (ab)^2$.

But if G is abelian, then $xy = a^2b^2 = (ab)^2$, $a, b \in G$. So, $xy \in H$.

Also, $x^{-1} = (a^2)^{-1} = (a^{-1})^2$.

Since $a^{-1} \in G$, so $x^{-1} \in H$.

Therefore, H is a subgroup of G only if G is abelian.

Theorem 5.3: Let H and K be two finite subgroups of a group G, then

$$o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)}$$

Proof: Let $N = H \cap K$. Then, N is a subgroup of H.

Therefore, H can be written as union of all distinct left cosets of N in H.

i.e., $$H = h_1N \cup h_2N \cup ... \cup h_rN \qquad ...(1)$$

where $h_i N$ are distinct left cosets of N in H.

Also, all these cosets have the same number of elements as N.

Thus, $$o(H) = o(h_1N) + o(h_2N) + ... + o(h_rN)$$

$$= \underbrace{o(N) + o(N) + ... + o(N)}_{r \text{ times}}$$

$$= r\,o(N)$$

Thus, $$r = \frac{o(H)}{o(N)} \qquad ...(2)$$

Now, $$HK = h_1NK \cup h_2NK ... \cup h_r NK \qquad \text{(from (1))}$$

$$= h_1K \cup h_2K ... \cup h_rK \qquad ...(3)$$

(Let $k \in K$, then $k = ek \in NK \Rightarrow K \subseteq NK$.

Also, $x \in NK \Rightarrow x = nk \in K$, as $n \in N \subseteq K$ and $k \in K$,

$\therefore$ $NK \subseteq K$ and so $NK = K$)

Now, let if possible, $h_iK = h_jK$ for $i \neq j$, then $h_i^{-1}h_j \in K$.

Also, $h_i^{-1}h_j \in H$.

Hence, $h_i^{-1}h_j \in N \Rightarrow h_iN = h_jN$, a contradiction

Therefore, all the above cosets are distinct. Thus, from (3),

$$\begin{aligned} o(HK) &= o(h_1K) + o(h_2K) + \ldots + o(h_rK) \\ &= o(K) + o(K) + \ldots + o(K) = r\,o(K) \\ &= \frac{o(H)\,o(K)}{o(H \cap K)} \qquad \text{(using (2))} \end{aligned}$$

Problem 5.11 Let G be a finite group and let H, K be subgroups of G such that $o(H) > \sqrt{o(G)}$ and $o(K) > \sqrt{o(G)}$. Show that $H \cap K \neq \{e\}$.

Solution We have, $o(G) \geq o(HK) = \dfrac{o(H)\,o(K)}{o(H \cap K)} > \dfrac{\sqrt{o(G)} \cdot \sqrt{o(G)}}{o(H \cap K)}$

This gives, $o(G) > \dfrac{o(G)}{o(H \cap K)}$. Therefore, $o(H \cap K) > 1$.

Hence, $H \cap K \neq \{e\}$.

Problem 5.12 If $o(G) = pq$, where p and q are primes, then prove that G can have at most one subgroup of order p.

Proof: Let H and K be two subgroups of G, each of order p. Let $p > q$.

We have $o(G) = pq < p^2$

Thus $\sqrt{o(G)} < p = o(H)$ and so $o(H) > \sqrt{o(G)}$

Similarly $o(K) > \sqrt{o(G)}$.

So, by previous problem, $H \cap K \neq \{e\}$.

But $H \cap K \leq H$ and $H \cap K \leq K$.

Therefore by Lagrange's Theorem,

$$o(H \cap K) \mid o(H) \text{ and } o(H \cap K) \mid o(K).$$

Thus $o(H \cap K) \mid p$ implying $o(H \cap K) = p$ or 1.

But $H \cap K \neq \{e\}$, therefore $o(H \cap K) \neq 1$.

Thus $o(H \cap K) = p = o(H) = o(K)$. Hence $H \cap K = H = K$.

Therefore $H = K$ and so G can have at most one subgroup of order p.

PROBLEM 5.13 Let G be a group of order 6 and let H, K be two distinct subgroups of G of order 2 each. Show that HK cannot be a subgroup of G.

SOLUTION We first show that $o(H \cap K) = 1$.

We know that $H \cap K$ is a subgroup of H.

Then, by Lagrange's Theorem, $o(H \cap K) | o(H) = 2$.

Therefore, $o(H \cap K) = 1$ or 2.

We assert that $o(H \cap K) \neq 2$.

Let, if possible, $o(H \cap K) = 2$, then $o(H \cap K) = o(H) = o(K)$.

Also, $H \cap K \subseteq H$ and $H \cap K \subseteq K$.

Thus, $H \cap K = H$ and $H \cap K = K$ implying $H = K$, which is a contradiction. Thus, o$(H \cap K) = 1$.

Consider, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = \dfrac{2.2}{1} = 4$.

But 4 does not divide 6 and so by Lagrange's Theorem, HK cannot be a subgroup of G.

PROBLEM 5.14 Show that a group of order 91 cannot have two different subgroups of order 13.

SOLUTION Given that $o(G) = 91$. Let H and K be two different subgroups of G of order 13.

Then, $H \cap K$ is a subgroup of H and so by Lagrange's Theorem,

$$o(H \cap K) | o(H) = 13.$$

This implies that $o(H \cap K) = 1$ or 13.

If $o(H \cap K) = 13$, then $H \cap K = H$. Similarly, $H \cap K = K$.

Thus, $H = K$, which is not true. Hence, $o(H \cap K) = 1$.

Now, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = \dfrac{13.13}{1} = 169 > o(G) = 91$, a contradiction.

So, we cannot have two different subgroups of order 13.

THEOREM 5.4: A group of prime order has no non-trivial subgroups.

Proof: Let $o(G) = p$, p is a prime and let H be any subgroup of G.

Then, by Lagrange's Theorem, $o(H) | o(G) = p$.

This implies, $o(H) = 1$ or p. Thus, $H = \{e\}$ or G.

Thus, group G has only trivial subgroups.

THEOREM 5.5: If G is a group of composite order, then it has at least one non-trivial subgroup.

Proof: Let $o(G) = n = rs$, where $1 < r, s < n$.

Let $a \in G$ be any element such that $a \neq e$.

Case I: If $a^r = e$, and if $o(a) = k$, we get $1 < k \leq r < n$.

Let $H = \{a, a^2, a^3, ..., a^k = e\}$ then, $o(H) = k$.

Since H is closed under multiplication, it is a subgroup of G and therefore it is the required subgroup.

Case II: If $a^r \neq e$, then $(a^r)^s = a^n = e$.

Let $o(a^r) = t$ and let $K = \{a^r, a^{2r}, a^{3r}, ..., a^{tr} = e\}$, $1 < t \leq s < n$.

Again, since K is closed under multiplication, therefore it is the required subgroup.

THEOREM 5.6: Let G be a group, which has no non-trivial subgroups. Then, $o(G)$ is prime.

Proof: We first prove that $o(G)$ cannot be infinite.

Suppose $o(G)$ is infinite. Let $a \in G$ be any element such that $a \neq e$.

Let H be the subgroup generated by a. Then, $H \neq \{e\}$.

Since G has no non-trivial subgroups, therefore $H = G$. Thus, $G = \langle a \rangle$.

Let $K = \langle a^2 \rangle$, then $K \neq \{e\}$, as if $K = \{e\}$ then $a^2 = e$ giving $o(a) \leq 2$,

which is not possible as $o(G)$ is infinite.

Hence $o(a)$ must be infinite.

Again $a \notin K$ as if $a \in \langle a^2 \rangle$ then $a = (a^2)^r$ implying $a^{2r-1} = e$.

$\Rightarrow$ $o(a) \leq 2r - 1$, a finite number, which is not true.

Thus $a \notin K$. Hence, $\{e\} \subset K \subset G$.

Therefore K is a non-trivial subgroup of G, which is a contradiction.

Hence $o(G)$ is finite. By previous theorem, $o(G)$ cannot be composite.

Hence it is a prime number.

PROBLEM 5.15 Show that if H and K are subgroups of a group G and $a \in G$, then $Ha \cap Ka = (H \cap K)a$.

SOLUTION Let $x \in Ha \cap Ka$. Then, $x \in Ha$ and $x \in Ka$.

$\Rightarrow$ $x = ha$ and $x = ka$ for some $h \in H$, $k \in K$

$\Rightarrow$ $ha = ka \Rightarrow h = k$, by right cancellation law in G.

Thus, $h \in H \cap K$ and $x = ha \Rightarrow x \in (H \cap K)a$.

$\therefore$ $Ha \cap Ka \subseteq (H \cap K)a$ ...(1)

Now, let $x \in (H \cap K)a$. Then, $x = ta$ for some $t \in H \cap K$

$\Rightarrow$ $x = ta$ for $t \in H$ and $x = ta$ for $t \in K$

$\Rightarrow$ $x \in Ha$ and $x \in Ka$

$\therefore$ $(H \cap K)a \subseteq Ha \cap Ka$. ...(2)

From (1) and (2), we get $Ha \cap Ka = (H \cap K)a$.

Problem 5.16 If G is a group and H, K are two subgroups of finite index in G, prove that $H \cap K$ is of finite index.

Solution Since H and K are two subgroups of G, therefore $H \cap K$ is a subgroup of G.

Also from the Problem 5.15, $Ha \cap Ka = (H \cap K)a$, $\forall a \in G$

Thus any right coset of $H \cap K$ is the intersection of a right coset of H and a right coset of K.

But, the number of such intersections is finite, since H and K are of finite index in G. Consequently, the number of right cosets of $H \cap K$ in G is finite.

Hence $H \cap K$ is of finite index.

Problem 5.17 Let a be an element of order 15. Find all the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.

Solution Let $G = \langle a \rangle$ and let $H = \langle a^5 \rangle$.

Since $o(a) = 15$, we have $a^{15} = e$.

Also $o(\langle a \rangle) = 15$ and so $o(\langle a^5 \rangle) = 3$.

Then $\langle a \rangle = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, a^{15} = e\}$

and $\langle a^5 \rangle = \{a^5, a^{10}, a^{15} = e\}$

By Lagrange's Theorem, number of distinct left cosets of H in G is given by $\dfrac{o(G)}{o(H)} = \dfrac{15}{3} = 5$.

And these cosets are

$$e\langle a^5 \rangle = \{a^5, a^{10}, e\} = a^5\langle a^5 \rangle = a^{10}\langle a^5 \rangle \quad (\because a \in H \Leftrightarrow aH = H)$$

$$a\langle a^5 \rangle = \{a^6, a^{11}, a\} = a^6\langle a^5 \rangle = a^{11}\langle a^5 \rangle$$

$$a^2\langle a^5 \rangle = \{a^7, a^{12}, a^2\} = a^7\langle a^5 \rangle = a^{12}\langle a^5 \rangle$$

$$a^3\langle a^5 \rangle = \{a^8, a^{13}, a^3\} = a^8\langle a^5 \rangle = a^{13}\langle a^5 \rangle$$

$$a^4\langle a^5 \rangle = \{a^9, a^{14}, a^4\} = a^9\langle a^5 \rangle = a^{14}\langle a^5 \rangle$$

Thus the distinct left cosets are $\langle a^5 \rangle$, $a\langle a^5 \rangle$, $a^2\langle a^5 \rangle$, $a^3\langle a^5 \rangle$ and $a^4\langle a^5 \rangle$

Problem 5.18 Use Lagrange's theorem, to prove that a finite group cannot be expressed as the union of two of its proper subgroups.

Solution Let G be a finite group of order n.

Suppose G is the union of two of its proper subgroups H and K.

Since e belongs to both H and K and $G = H \cup K$, therefore at least one of H and K (say H) must contain more than half the elements of G.

Let $o(H) = p$.

Then, $\frac{n}{2} < p < n$. (As H is a proper subgroup of G)

Since $\frac{n}{2} < p < n$, therefore p cannot be a divisor of n.

This contradicts Lagrange's theorem, which states that the order of each subgroup of a finite group is a divisor of the order of the group.

Hence our assumption is wrong and so a finite group cannot be expressed as the union of two of its proper subgroups.

Problem 5.19 Suppose that $o(G) = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

Solution Let H be a proper subgroup of G, then by Lagrange's Theorem, $o(H) \mid o(G) = pq$.

Therefore, $o(H) = 1$, p or q.

Case I: If $o(H) = 1$, then $H = \{e\}$. Thus, H is cyclic.

Case II: If $o(H) = p$, then there exists $a \in H$ such that $a \neq e$.

By Corollary of Lagrange's Theorem, $o(a) \mid o(H)$.

Thus, $o(\langle a \rangle) \mid o(H)$. Therefore, $o(\langle a \rangle) = 1$ or $o(\langle a \rangle) = p$.

If $o(\langle a \rangle) = 1$, then $a = e$, a contradiction (as $a \neq e$)

Thus $o(\langle a \rangle) = p$. We know, $\langle a \rangle$ is a subgroup of H and $o\langle a \rangle = p$, therefore $H = \langle a \rangle$.

Hence H is cyclic.

Case III: If $o(H) = q$, then as discussed above, we have H is cyclic.

Thus from all the cases, we see that H is cyclic.

Problem 5.20 If H is a subgroup of G such that whenever $Ha \neq Hb$, then $aH \neq bH$. Prove that $gHg^{-1} \subseteq H$ for all $g \in G$.

Solution The condition $Ha \neq Hb \Rightarrow aH \neq bH$ is equivalent to the following condition

$$aH = bH \Rightarrow Ha = Hb \qquad ...(1)$$

We have $gHg^{-1} = \{ghg^{-1} : h \in H\}$

Let $g \in G$ and $h \in H$, then $(g^{-1}h)H = g^{-1}(hH) = g^{-1}H$ (as $h \in H$)

Using (1), $(g^{-1}h)H = g^{-1}H$ implies $H(g^{-1}h) = Hg^{-1}$

Thus $(g^{-1}h)(g^{-1})^{-1} \in H$, giving $g^{-1}hg \in H$, $\forall\ g \in G, h \in H$

Therefore $g^{-1}Hg \subseteq H$, $\forall\ g \in G$ ...(2)

Hence $gHg^{-1} = (g^{-1})^{-1}H(g^{-1}) \subseteq H$ for all $g \in G$, using (2).

Problem 5.21 Let $o(G) = 15$. If G has only one subgroup of order 3 and only one subgroup of order 5, prove that G is cyclic.

Solution Let H be a subgroup of G of order 3 and K be a subgroup of G of order 5.

Let $a \in G$ be such that $a \notin H \cup K$.

By Lagrange's Theorem, $o(a) = 3$, 5 or 15.

But $o(a) \neq 3$, as if $o(a) = 3$, then $H = \langle a \rangle$ and so $a \in H$, which is not true.

Also $o(a) \neq 5$, as if $o(a) = 5$, then $K = \langle a \rangle$ and so $a \in K$, which is not true.

Thus $o(a) = 15$. Also, $o(G) = 15$.

Therefore $G = \langle a \rangle$ is cyclic.

Problem 5.22 Let G be a cyclic group of order 6 generated by a. If $H = \langle a^2 \rangle$ and $K = \langle a^3 \rangle$, show that $G = HK$.

Solution We have, $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$

Then $H = \{a^2, a^4, a^6 = e\}$ and $K = \{a^3, a^6 = e\}$.

Thus $o(H) = 3$, $o(K) = 2$ and $H \cap K = \{e\}$.

Since G is cyclic, G is abelian and so HK is a subgroup of G.

Now $o(HK) = \dfrac{o(H)\,o(K)}{o(H \cap K)} = \dfrac{2.3}{1} = 6 = o(G)$.

Hence $G = HK$, as HK is a subgroup of G.

Problem 5.23 Suppose that G is an abelian group with an odd number of elements. Show that the product of all the elements of G is the identity.

Solution Since G has odd order, no element of G can have order 2.

Thus for each $x(\neq e) \in G$, we have $x \neq x^{-1}$.

So we can write the product of all the elements in the form

$$ea_1 \times a_1^{-1} \times a_2 \times a_2^{-1} \times \ldots \ldots a_n \times a_n^{-1} = e$$

Problem 5.24 Show that the set of the inverses of the elements of a right coset is a left coset or more precisely, show that $(Ha)^{-1} = a^{-1}H$.

Solution Suppose Ha is a right coset of H in G, where $a \in G$.

Let ha be any element of Ha, where $h \in H$.

We have $(ha)^{-1} = a^{-1}\, h^{-1}$.

Since H is a subgroup, therefore $h \in H$ gives $h^{-1} \in H$.

Therefore $a^{-1}h^{-1} \in a^{-1}H$.

Thus inverses of all the elements of Ha belong to the left coset $a^{-1}H$.

Hence $(Ha)^{-1} \subseteq a^{-1}H$.

Conversely, let $a^{-1}h$ be any element of $a^{-1}H$.

Then $a^{-1}h = a^{-1}(h^{-1})^{-1} = (h^{-1}a)^{-1} \in (Ha)^{-1}$, since $h^{-1} \in H$.

Therefore every element of $a^{-1}H$ belongs to the set of the inverses of the elements of Ha.

Thus $a^{-1}H \subseteq (Ha)^{-1}$.

Hence $(Ha)^{-1} = a^{-1}H$.

Problem 5.25 Show that a group of order $2p$, where p is prime and $p > 2$, has exactly one subgroup of order p.

Solution Suppose G has two distinct subgroups H and K such that

$$o(H) = o(K) = p.$$

By Lagrange's Theorem, $o(H \cap K)$ divides $o(H) = p$.

$\Rightarrow$ $o(H \cap K) = 1$ or p, since p is prime.

If $o(H \cap K) = p$, then $o(H \cap K) = o(H)$ or $H \cap K = H$. Similarly $H \cap K = K$.

Thus, $H = K$, which is a contradiction. Therefore, $o(H \cap K) = 1$.

We have, $o(HK) = \dfrac{o(H)\, o(K)}{o(H \cap K)} = \dfrac{p.p}{1} = p^2 > o(G) = 2p,$ since $p > 2$ and p is prime.

So, $o(HK) > o(G)$ which is not possible.

Hence, G has exactly one subgroup of order p.

Problem 5.26 Prove that the only right (or left) coset of a subgroup H in a group G, which is also a subgroup of G, is H itself.

Solution Suppose Ha is a right coset of H in G.

Let Ha be a subgroup of G. Then, $e \in Ha$. But $e \in H$.

Since H is itself a right coset and two right cosets are either disjoint or identical, therefore $H = Ha$.

Similarly aH is a subgroup of G implies $aH = H$.

The following problem gives a geometrical picture of cosets of a subgroup in some groups.

Problem 5.27 Let G be the group of non-zero complex numbers under multiplication and let $H = \{x \in G : |x| = 1\}$. Give a geometrical description of the cosets of H.

Solution The set H represents a unit circle centred at the origin.

Let $a \in G$ be any element. Then, $aH = \{ah : h \in H\}$.

We shall show that $aH = \{z \in G : |z| = |a|\}$

Now, $x \in aH \Leftrightarrow x = ah$, for some $h \in H$

$\Leftrightarrow a^{-1}x = h \in H$

$\Leftrightarrow |a^{-1}x| = |h| = 1$

$\Leftrightarrow |x| = |a|$

$\Leftrightarrow x \in \{z \in G : |z| = |a|\}$

$\Leftrightarrow x$ lies on the circle centred at origin and radius $|a|$.

Therefore, aH is the set of all points on a circle with centre at origin and radius $|a|$.

Thus the cosets are nothing but concentric circles centred at origin.

Problem 5.28 Show that $\mathbb{Q}$, the group of rational numbers under addition, has no proper subgroup of finite index.

Solution Let x be any non-zero rational number.

Suppose there are n distinct cosets of some proper subgroup H of $\mathbb{Q}$.

Consider the $n + 1$ cosets H, $x + H$, $2x + H$, ... , $nx + H$.

Since there are only n different cosets of H in $\mathbb{Q}$, two of these $n + 1$ cosets must be equal, say, $ix + H = jx + H$ with $j > i$.

Then $(j - i)x + H = H$, where $0 < j - i < n$.

Thus $(j - i)x \in H$.

Since $j - i$ is a factor of $n!$, so by closure $n!\, x \in H$.

Thus for every rational number x, we have $n!\, x \in H$.

That means $n!Q$ is a subset of H.

But $n!Q = \{n!\, x : x \in Q\} = Q$

(as for any positive integer k, the set $kQ = \{kx : x \in Q\} = Q$)

So we have proved that Q is a subset of H. That means H is not a proper subgroup of Q.

Problem 5.29 Prove that a non-abelian group of order 10 must have five elements of order 2.

Solution Let G be a non-abelian group of order 10.

Since the order of an element divides the order of the group, the possible orders of the elements of G are 1, 2, 5 and 10.

Clearly e is the only element of order 1.

Also G has no element of order 10, because if G has an element of order 10, then G is cyclic (as $o(G) = 10$) and therefore abelian, which is a contradiction to the hypothesis that G is non-abelian.

Also every element of G cannot be of order 2, because if every element is of order 2, then G must be abelian, a contradiction, as G is non-abelian.

Therefore there exists an element $a \in G$ such that $o(a) = 5$.

Let $H = \langle a \rangle$. Then, as $o(H) = 5$, we have $i_G(H) = \dfrac{o(G)}{o(H)} = 2$.

Let $c \notin H$. Then, $G = H \cup cH$. Since, $c^2 \in G = H \cup cH$,

Therefore $c^2 \in H$ or $c^2 \in cH$.

Now $c^2 \in cH \Rightarrow c^2 = ch$, for some $h \in H \Rightarrow c = h$ for some $h \in H$, a contradiction to the choice of c. Therefore, $c^2 \notin cH$.

So $c^2 \in H$. Then, $o(c^2) = 1$ or 5 as $o(c^2)$ divides $o(H) = 5$

Now $o(c^2) = 5 \Rightarrow o(c) = 10$, which contradicts that G has no element of order 10.

Therefore $o(c^2) = 1$ implying $o(c) = 2$.

Since there are 5 elements of G which are not in H, therefore there are 5 elements of order 2 in G.

Problem 5.30 Prove that an abelian group of order $2p$, where p is an odd prime, must have one element of order 2.

Solution Let G be an abelian group of order $2p$, where p is an odd prime.

We first prove that G has an element of order 2.

Two cases arise:

Case I: G has an element of order $2p$, say a.

Then $o(a) = 2p \Rightarrow o(a^p) = 2$, so that a^p is an element of order 2.

Case II: G has no element of order $2p$.

Let $x \in G$ and $x \neq e$. Then, $o(x) = 2$ or p.

If $o(x) = 2$, then we are done.

If $o(x) = p$ let $H = \langle x \rangle$. Then, $o(H) = p$, so that $i_G(H) = 2$.

Hence there exists $b \notin H$ such that $G = H \cup Hb$.

Since $b \notin H$, $b^2 \notin Hb$, so that $b^2 \in H$. Then, $o(b^2) = 1$ or $o(b^2) = p$

But $o(b^2) = p$ gives $o(b) = 2p$, which contradicts our assumption that G has no element of order $2p$.

Therefore $o(b^2) = 1$, so that $b^2 = e$. Hence, $o(b) = 2$.

Thus b is the required element of order 2.

Uniqueness: Let, if possible, there exists two distinct elements x and y of order 2 and let $H = \langle x \rangle$ and $K = \langle y \rangle$.

Then $H = \{e, x\}$ and $K = \{e, y\}$. Therefore, $H \cap K = \{e\}$.

Since G is abelian, $HK = KH$ so that HK is a subgroup of G and

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = 4.$$

But G cannot have a subgroup of order 4 because 4 does not divide $o(G) = 2p$, where p is odd prime.

So our assumption is wrong. Thus, there is a unique element of order 2.

Problem 5.31 Suppose H and K are subgroups of a group G. If $o(H) = 12$ and $o(K) = 35$, find $o(H \cap K)$.

Solution Since $o(H \cap K) \mid o(H)$ and $o(H \cap K) \mid o(K)$,

we get, $o(H \cap K) \mid 12$ and $o(H \cap K) \mid 35$.

Since gcd(12, 35) = 1, therefore $o(H \cap K) = 1$.

Problem 5.32 Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $|G : H| = |G : K|\,|K : H|$.

Solution We have $|G : H| = \dfrac{o(G)}{o(H)}$, $|G : K| = \dfrac{o(G)}{o(K)}$, $|K : H| = \dfrac{o(K)}{o(H)}$.

So, $$|G : K|\,|K : H| = \frac{o(G)}{o(K)} \cdot \frac{o(K)}{o(H)} = \frac{o(G)}{o(H)} = |G : H|\ .$$

5.3 Application of Cosets to Permutation Groups

We now consider an application of cosets to permutation groups.

Definition 5.3: Let G be a group of permutations of a set A.

For each $i \in A$, define

$$\text{stab}_G(i) = \{\varphi \in G : \varphi(i) = i\}$$

It is the set of all those permutations in G which fixes i.

The set $\text{stab}_G(i)$ is called the **stabilizer of the point *i* in *G*.**

Definition 5.4: Let G be a group of permutations of a set A.

For each $i \in A$, define, $\text{orb}_G(i)$ called **orbit of the point *i* under *G*** to be the set

$$\text{orb}_G(i) = \{\varphi(i) : \varphi \in G\}$$

This is the set of all the images of i in every permutation in G.

Theorem 5.7: Stabilizer of an element in a group G of permutations is a subgroup of G.

Proof: Let G be a group of permutations of a set A. Let $i \in A$.

Let $S = \text{stab}_G(i) = \{\varphi \in G : \varphi(i) = i\}$. Then $S \neq \phi$ as $I \in S$

Next, let $f, g \in S$ then $f(i) = i$ and $g(i) = i$.

Therefore $f \circ g(i) = f(g(i)) = f(i) = i, \forall\ i \in G$

So $f \circ g \in S$.

Again, let $f \in S$ then $f(i) = i$. Since f is a permutation, it is bijective and hence f^{-1} exists and $f^{-1}(i) = i$, so $f^{-1} \in S$.

Therefore S is a subgroup of G.

Example 5.7: Let $G = \{(1), (132)(465)(78), (132)(465), (123)(456), (123)(456)(78), (78)\}$

Then

1. $\text{orb}_G(1) = \{1, 3, 2\}$
2. $\text{orb}_G(2) = \{2, 1, 3\}$
3. $\text{orb}_G(4) = \{4, 6, 5\}$
4. $\text{orb}_G(7) = \{8, 7\}$
5. $\text{stab}_G(1) = \{(1), (78)\}$
6. $\text{stab}_G(2) = \{(1), (78)\}$
7. $\text{stab}_G(4) = \{(1), (78)\}$
8. $\text{stab}_G(7) = \{(1), (132)(465), (123)(456)\}$

Note: For the sake of convenience, for a fix i, we let $\text{stab}_G(i) = S$ and $\text{orb}_G(i) = O_i$.

We now prove the theorem, called **Orbit Stabilizer Theorem.**

Theorem 5.8: Let G be a finite group of permutations of a set A.

Then for any a in A,

$$o(G) = o(\text{stab}_G(a)) \cdot o(\text{orb}_G(a))$$

Proof: Fix an element $a \in A$.

Let $S = \text{stab}_G(a) = \{\varphi \in G : \varphi(a) = a\}$

and $O_a = \text{orb}_G(a) = \{\varphi(a) : \varphi \in G\}$

To show: $o(G) = o(S) \cdot o(O_a)$.

Since S is a subgroup of G, by Lagrange's theorem we have

$$\frac{o(G)}{o(S)} = i_G(S).$$

Thus we only need to show that $i_G(S) = o(O_a)$, i.e., the number of distinct left cosets of S in G is equal to the number of elements in the orbit of a.

Let H be the set of all left cosets of S in G, i.e., $H = \{\alpha S : \alpha \in G\}$.

So now we have to show that $o(H) = o(O_a)$.

Define a map $T : H \to O_a$ as $T(\alpha S) = \alpha(a)$.

Then T is well-defined and one-one as

$$\begin{aligned} & \alpha S = \beta S \\ \Leftrightarrow \quad & \alpha^{-1}\beta \in S \\ \Leftrightarrow \quad & (\alpha^{-1}\beta)(a) = a \\ \Leftrightarrow \quad & (\alpha^{-1}(\beta(a))) = a \\ \Leftrightarrow \quad & \beta(a) = \alpha(a) \\ \Leftrightarrow \quad & T(\alpha S) = T(\beta S) \end{aligned}$$

We now prove that T is onto.

Let $c \in O_a$ then, $c = \varphi(a)$ for some $\varphi \in G$.

Therefore $c = \varphi(a) = T(\varphi S)$. Thus, T is onto.

Hence T is a bijection and hence $o(H) = o(O_a)$ and so the result.

Problem 5.33 Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$

(a) Find the stabilizer of 1 and the orbit of 1.

(b) Find the stabilizer of 3 and the orbit of 3.

(c) Find the stabilizer of 5 and the orbit of 5.

Solution

(a) $\text{stab}_G 1 = \{(1), (24)(56)\}$; $\text{orb}_G 1 = \{1, 2, 3, 4\}$

(b) $\text{stab}_G 3 = \{(1), (24)(56)\}$; $\text{orb}_G 3 = \{3, 4, 1, 2\}$

(c) $\text{stab}_G 5 = \{(1), (12)(34), (13)(24), (14)(23)\}$; $\text{orb}_G 5 = \{5, 6\}$

Exercises

1. If G is a group of order 35, show that it cannot have two subgroups of order 7.

2. Suppose that a has order 30. Find all the left cosets of $\langle a^4 \rangle$ in $\langle a \rangle$.

3. Let $G = D_4$ with $A = \{1, 2, 3, 4\}$. Find the orbit and stabilizer of each element of A.

4. Prove that in a subgroup of index 3 every left coset may not be a right coset.

5. Let G be a group such that $o(G) = 77$. Prove that every proper subgroup of G is cyclic.

6. Let H, K be subgroups of a group. If $o(H) = 24$ and $o(K) = 55$, find the order of $H \cap K$.

7. Let G be a group with an odd number of elements. Prove that $a^2 \neq e$ for each non identity $a \in G$.

8. Suppose that H, K are subgroups of a group G such that $L = H \cap K \neq \{e\}$. Suppose $o(H) = 14$ and $o(K) = 35$. Find $o(L)$.

9. Let $G = \langle a \rangle$ and $o(a) = 30$. Find the index of $\langle a^6 \rangle$ in G.

10. Show that $o(\mathbb{Z}_n^*)$ under multiplication modulo n is even for $n \geq 3$.

11. Find all left and right cosets of $(3\mathbb{Z}, +)$ in $(\mathbb{Z}, +)$.

Hints to selected problems

5. Since $o(G) = 77 = (7)(11)$ is a product of two primes, every proper subgroup of G is cyclic by problem 5.19.

6. Since $H \cap K$ is a subgroup of both H and K, $o(H \cap K)$ divides both $o(H)$ and $o(K)$. Since gcd(24, 55) = 1 and $o(H \cap K)$ divides both numbers 24 and 55, therefore $o(H \cap K) = 1$. Thus, $H \cap K = \{e\}$.

7. Suppose that $a^2 = e$ for some non-identity $a \in G$. Then, $\{e, a\}$ is a subgroup of G of order 2. Hence, 2 divides $o(G)$. A contradiction as 2 is an even integer and $o(G)$ is an odd integer.

8. Since L is a subgroup of both H and K, $o(L)$ divides both 14 and 35. Since 1 and 7 are the only numbers that divide both 14 and 35 and $H \cap K \neq \{e\}$, $o(L) \neq 1$. Hence, $o(L) = 7$.

Check for updates

6

Normal Subgroups and Factor Groups

Learning Objectives

- Normal Subgroups and Equivalent Conditions for a Subgroup to be Normal
- Factor Groups (Quotient Groups)
- Commutator Subgroup of a Group and its Properties
- The G/Z Theorem
- Cauchy's Theorem for Abelian Groups

6.1 Normal Subgroup and Equivalent Conditions for a Subgroup to be Normal

We will define a special class of subgroups called normal subgroups and also known as invariant subgroups or self-conjugate subgroups. Évariste Galois† was the first mathematician to recognize the importance of the existence of normal subgroups. Normal subgroups are used to form Factor groups of the given group, which we shall study in detail in section 6.2. We will also find equivalent conditions for a subgroup to be normal.

Definition 6.1: A subgroup H of a group G is called a **normal subgroup** of G if $gH = Hg$, for all $g \in G$, i.e., there is no distinction between left and right cosets for a normal subgroup.

Note that $H \trianglelefteq G$ means H is a normal subgroup of G.

Also note that $gH = Hg$ does not mean that $hg = gh$ for all $g \in G$ and $h \in H$. It only means that if $g \in G$ and $h \in H$, then there exists some $h_1 \in H$ such that $hg = gh_1$.

† Évariste Galois was a French mathematician, born in Bourg-la-Reine, who revolutionized mathematics. Galois possessed an extraordinary brilliance in mathematics. His most noteworthy contribution to the discipline is his development of Galois Theory. He died tragically young, at the age of 20, not in the cause of mathematics, but for reasons that forged a grand myth of a romantic genius.

© The Author(s) 2023
D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_6

Example 6.1: Let G be the quaternion group, $G = \{\pm 1, \pm i, \pm j, \pm k\}$

such that $i^2 = j^2 = k^2 = -1$

and $ij = k = -ji, jk = i = -kj, ki = j = -ik.$

Let $H = \{1, -1\}$. Then, H is a subgroup of G.

Also $Ha = \{a, -a\} = aH, \ \forall a \in G.$

Therefore H is a normal subgroup of G.

Definition 6.2: Every group G possesses at least two normal subgroups, namely, G itself and the subgroup $\{e\}$ consisting of the identity element e alone.

These are called the **improper normal subgroups**.

Note that there exist groups for which these are the only normal subgroups.

Such groups are known as **simple groups**. We define it as follows:

Definition 6.3: A **simple group** G is a group whose only normal subgroups are $\{e\}$ and G.

There are several equivalent definitions of normal subgroup. To verify that a subgroup is normal, it is usually better to use the following theorem:

Theorem 6.1: A subgroup H of a group G is normal in G if and only if $xHx^{-1} \subseteq H$, for all $x \in G$.

Proof: Let H be a normal subgroup of G.

Then $xH = Hx, \ \forall x \in G$. Thus, $xHx^{-1} = Hxx^{-1} = H$.

In particular, $xHx^{-1} \subseteq H, \forall x \in G$.

Conversely, let $xHx^{-1} \subseteq H, \forall x \in G$. To show that $xH = Hx$.

Since $xHx^{-1} \subseteq H$ we have $xH \subseteq Hx$ ...(1)

Also $x^{-1}H(x^{-1})^{-1} \subseteq H$ as $x^{-1} \in G$.

$\Rightarrow x^{-1}Hx \subseteq H$.

$\Rightarrow Hx \subseteq xH$ ...(2)

Therefore from (1) and (2) we have $xH = Hx \ \forall x \in G$ and thus H is normal in G.

Remark: Clearly, it makes no difference in the argument if the above condition is read as $x^{-1}Hx \subseteq H \ \forall x \in G$.

Theorem 6.2: Every subgroup of an abelian group is normal.

Proof: Let H be a subgroup of an abelian group G.

To show that H is normal in G, we need to prove that $xHx^{-1} \subseteq H, \ \forall x \in G$.

Let $x \in G$ and $h \in H$ be arbitrary elements.

Then $xhx^{-1} = (xh)x^{-1} = (hx)x^{-1}$, $x \in G$ (since $h \in H \leq G$ and G is abelian)

Thus $xhx^{-1} = h(xx^{-1}) = he = h \in H, \forall x \in G$

Therefore $xHx^{-1} \subseteq H, \forall x \in G$ and hence H is a normal subgroup of G.

Theorem 6.3: The center $Z(G)$ of a group G is always normal.

Proof: We have $Z(G) = \{h \in G : hx = xh \ \forall x \in G\}$

We know $Z(G)$ is a subgroup of G.

Now let $x \in G$ and $h \in Z(G)$ be arbitrary elements.

Then $xhx^{-1} = (xh)x^{-1} = (hx)x^{-1}$ (since $h \in Z(G)$ and $x \in G$)

$= h(xx^{-1}) = he = h \in Z(G)$

Therefore, $xZ(G)x^{-1} \subseteq Z(G), \forall x \in G$ and so, $Z(G)$ is a normal subgroup of G.

Theorem 6.4: A subgroup of G of index 2 is a normal subgroup of the group G.

Proof: Let G be a group and H be a subgroup of G such that $i_G(H) = 2$.

Then there are only two distinct left (right) cosets of H in G and G can be expressed as union of these two left (right) cosets.

To prove that H is a normal subgroup of G, we need to show that

$$gH = Hg, \forall g \in G.$$

Case I: Let $g \in H$. Then $gH = H = Hg$.

Therefore $gH = Hg$ and so H is a normal subgroup of G.

Case II: Let $g \notin H$, then $gH \neq H$ and $Hg \neq H$.

Thus H and gH are two distinct left cosets of H in G and $G = H \cup gH$.

Further H and Hg are two distinct right cosets of H in G and $G = H \cup Hg$.

Therefore $H \cup gH = H \cup Hg$.

Also since two left(right) cosets are either identical or disjoint, we have

$$H \cap gH = \phi = H \cap Hg.$$

Therefore $gH = Hg$ and hence H is a normal subgroup of G.

Remark: The converse of the result, "A subgroup of index 2 is a normal subgroup", need not hold, as shown in the following example:

Example 6.2: Let $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with

$$i^2 = j^2 = k^2 = -1, \ ij = k = -ji, \ jk = i = -kj, \ ki = j = -ik.$$

Let $H = \{1, -1\}$. Then, H being the center of Q_8 is normal in Q_8.

But $i_G(H) = \dfrac{o(G)}{o(H)} = \dfrac{8}{2} = 4 \neq 2$.

THEOREM 6.5: A subgroup H of a group G is normal if and only if the product of two right cosets of H in G is a right coset of H in G.

Proof: Let H be a normal subgroup of a group G.

Let Ha and Hb be any two right cosets of H in G.

Then $(Ha)(Hb) = H(aH)b = H(Ha)b$ $(\because H \trianglelefteq G)$

$= HH(ab) = H(ab)$

Thus product of two right cosets is again a right coset.

Conversely, let the given condition holds.

Let $g \in G$ be any element, then $g^{-1} \in G$ and Hg and Hg^{-1} are two right cosets.

By given condition, $(Hg)(Hg^{-1})$ is a right coset.

Now $egeg^{-1} \in HgHg^{-1}$, so $e \in HgHg^{-1}$. Also, $e \in H = He$.

Thus, e is a common element in the two right cosets $HgHg^{-1}$ and H.

Since two right cosets are either equal or have nothing in common,

Hence $HgHg^{-1} = H$ …(1)

Now $h_1ghg^{-1} \in HgHg^{-1} \; \forall \; h, h_1 \in H$

$\Rightarrow$ $h_1ghg^{-1} \in H \; \forall \; h, h_1 \in H$ (Using (1))

$\Rightarrow$ $ghg^{-1} \in h_1^{-1}H \; \forall \; h \in H$

$\Rightarrow$ $ghg^{-1} \in H \; \forall \; h \in H, g \in G$ $(\because Ha = H \text{ if } a \in H)$

Thus H is a normal subgroup of G.

PROBLEM 6.1 Give an example of a non–abelian group each of whose subgroups are normal.

SOLUTION Let $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with

$$i^2 = j^2 = k^2 = -1, \; ij = k = -ji, \; jk = i = -kj, \; ki = j = -ik.$$

We know that G is non-abelian. Let H be a subgroup of G.

By Lagrange's theorem $o(H) \mid o(G) = 8$.

Thus $o(H) = 1, 2, 4$ or 8.

If $o(H) = 1$ or 8, then H is trivially a normal subgroup of G.

If $o(H) = 4$, then $i_G(H) = 2$ and a subgroup of index 2 is always normal.

Now let $o(H) = 2$, then $H = \{1, -1\}$, which being the center of Q_8, is normal.

Thus every subgroup of Q_8 is normal.

PROBLEM 6.2 A subgroup H of a group G is normal in G if and only if $g^{-1}hg \in H$ for all $h \in H$, $g \in G$.

SOLUTION Let $g^{-1}hg \in H$, for all $h \in H$ and $g \in G$.

Then $g^{-1}Hg \subseteq H$ and hence H is normal in G.

Other way, let H be normal in G then $g^{-1}Hg \subseteq H$ for all $g \in G$.

Thus $g^{-1}hg \in H$, for all $h \in H$ and $g \in G$.

PROBLEM 6.3 Give an example of three groups $E \subset F \subset G$, where E is normal in F, F is normal in G, but E is not normal in G.

SOLUTION We consider three subgroups of S_4 as follows:

$E = \{I, (12)(34)\}$

$F = \{I, (12)(34), (13)(24), (14)(23)\}$

$G = \{I, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$

Clearly $E \subset F \subset G$.

Also $i_G(F) = \dfrac{o(G)}{o(F)} = \dfrac{8}{4} = 2$. Therefore F is normal in G.

Also $i_F(E) = \dfrac{o(F)}{o(E)} = \dfrac{4}{2} = 2$. Therefore E is normal in F

But E is not nomal in G as let $g = (1234) \in G$ and $n = (12)(34) \in E$.

Then $gng^{-1} = (1234)(12)(34)(4321) = (14)(23) \notin E$.

PROBLEM 6.4 Let H and K be subgroups of a group G. Prove that if one of them is normal, then HK is a subgroup of G and if both of them are normal, then HK is a normal subgroup of G.

SOLUTION Let H be normal in G and K be a subgroup of G.

Since H is normal in G, therefore, $Hg = gH$, $\forall g \in G$.

In particular, $Hk = kH$, $\forall k \in K$

Thus $HK = KH$ and so HK is a subgroup of G.

Now let H and K be normal subgroups of the group G.

To show: HK is a normal subgroup of G.

Clearly HK is a subgroup of G.

Now let $g \in G$ and $a \in HK$ be any arbitrary elements.

Then $a \in HK$ implies $a = hk$ for some $h \in H$, $k \in K$.

Therefore $g^{-1}\, ag = g^{-1}\, hkg = g^{-1}h(gg^{-1})\, kg = (g^{-1}hg)(g^{-1}kg) \in HK$.

Hence HK is a normal subgroup of G.

Problem 6.5 Show that the intersection of two normal subgroups of a group G is a normal subgroup of G.

Solution Let H and K be normal subgroups of a group G.

Let $x \in H \cap K$ and let $g \in G$. Then $x \in H$ and $x \in K$.

Therefore $gxg^{-1} \in H$ and $gxg^{-1} \in K$.

Thus $gxg^{-1} \in H \cap K$ for all $g \in G$.

Hence $H \cap K$ is normal in G.

Problem 6.6 If H and K are normal subgroups of a group G such that $H \cap K = \{e\}$, then prove that $hk = kh$, $\forall h \in H$, $\forall k \in K$.

Solution Let $h \in H$ and $k \in K$ be any arbitrary elements.

Since H is a normal subgroup of G and $k \in K \subseteq G$, therefore $k^{-1} hk \in H$.

Thus $h^{-1}k^{-1}hk \in H$ ($\because h^{-1} \in H$ and by closure) ...(1)

Again, K is a normal subgroup of G and $h \in H \subseteq G$,

therefore $h^{-1}k^{-1}h \in K$ ($\because k \in K \Rightarrow k^{-1} \in K$ as $K \leq G$)

So $h^{-1} k^{-1} hk \in K$ ...(2)

From (1) and (2), we get $h^{-1}k^{-1}hk \in H \cap K = \{e\}$

Thus $h^{-1}k^{-1}hk = e$ giving $k^{-1}hk = h$ and hence $hk = kh$, $\forall h \in H$, $\forall k \in K$.

Problem 6.7 Let N be a normal subgroup of a group G with order 2. Show that N is contained in $Z(G)$.

Solution: We have, $o(N) = 2$. Let $N = \{e, a\}$.

To prove that $N \subseteq Z(G) = \{a \in G : ag = ga \ \forall g \in G\}$

Clearly, $e \in Z(G)$. We now show that $a \in Z(G)$.

Let $g \in G$ be any element.

Since $a \in N$ and N is a normal subgroup of G, we have $g^{-1}ag \in N$.

Then $g^{-1}ag = e$ or $g^{-1}ag = a$.

If $g^{-1}ag = e$ then $ag = ge = eg$ giving $a = e$, which is not true.

Hence $g^{-1}ag = a$ implying $ag = ga$, $\forall g \in G$.

So, $a \in Z(G)$ and hence N is contained in $Z(G)$.

Problem 6.8 Prove that if G is a finite group and H is the only subgroup of order $o(H)$, then H is normal in G.

Proof: Let $g \in G$ be any element.

Define a mapping $f : H \to g^{-1} Hg$ such that $f(h) = g^{-1} hg$

Then, $h_1 = h_2 \Leftrightarrow g^{-1}h_1g = g^{-1}h_2g \Leftrightarrow f(h_1) = f(h_2)$

Therefore the mapping f is well defined and one-one.

Clearly f is onto. Therefore $o(H) = o(g^{-1}Hg)$

By the given condition, $H = g^{-1}Hg$. Thus, $gH = Hg$, $\forall g \in G$.

Therefore, H is a normal subgroup of G.

Problem 6.9 Let H be a subgroup of a group G such that $x^2 \in H$, $\forall x \in G$. Show that H is a normal subgroup of G.

Proof: Let $g \in G$ be any element. Let $h \in H$.

Then, $gh \in G$ ($\because H \leq G$, so $h \in H \subseteq G \Rightarrow h \in G$)

Thus, by given condition $(gh)^2 \in H$.

This gives $ghgh \in H$. ...(1)

Again $g \in G$ implies $g^{-1} \in G$. So $g^{-2} \in H$. ...(2)

From (1) and (2), we get

$$g^{-2}(ghgh) \in H.$$

Thus $g^{-1}hgh \in H$ and so $g^{-1}hg \in Hh^{-1} = H$

Therefore $g^{-1}hg \in H$ and hence H is a normal subgroup of G.

Problem 6.10 Let G be a group and N be a normal subgroup of G. If N is cyclic, show that all subgroups of N are normal in G.

Solution Since N is cyclic, let us suppose that $N = \langle a \rangle$.

Let H be any subgroup of N. We have to show that H is a normal subgroup of G.

Since H is a subgroup of a cyclic group, therefore H will be cyclic.

Let $H = \langle a^m \rangle$, $m \in \mathbb{Z}$, Let $g \in G$ and $h \in H$ be any elements.

Then $h = (a^m)^n$ for some $n \in \mathbb{Z}$.

Therefore $g^{-1}hg = g^{-1}(a^m)^n g = g^{-1}(a^n)^m g = (g^{-1}a^n g)^m$.

As N is cyclic and $N = \langle a \rangle$, so, $a^n \in N$.

Again as N is normal in G, we get $g^{-1}a^n g \in N = \langle a \rangle$.

Thus $g^{-1}a^n g = a^t$ for some $t \in Z$.

Therefore $(g^{-1}a^n g)^m = (a^t)^m$ implies $g^{-1}hg = (a^m)^t \in H$,

i.e., $g^{-1}hg \in H$ and hence H is a normal subgroup of G.

Problem 6.11 Prove that a subgroup H of a group G is normal in G if and only if $Ha \neq Hb$ implies $aH \neq bH$, $\forall\, a, b \in G$.

Solution Let H be a normal subgroup of G and $Ha \neq Hb$.

Since H is normal in G, we have $Ha = aH$ and $Hb = bH$

Thus, $aH \neq bH$.

Conversely, let $Ha \neq Hb$ implies $aH \neq bH$

Then, $aH = bH$ gives $Ha = Hb$

i.e., $a^{-1}b \in H$ gives $ab^{-1} \in H$ ...(1)

Now let $g \in G$ and $h \in H$ be any elements.

Then, $h^{-1} \in H$ implies $h^{-1}g^{-1}g \in H$. So, $(gh)^{-1}\, g \in H$

Using (1), we have $ghg^{-1} \in H$ and hence H is a normal subgroup of G.

Problem 6.12 Prove that all subgroups of a cyclic group are normal.

Solution We have every subgroup of a cyclic group is cyclic. Also, every cyclic group is abelian and every subgroup of an abelian group is normal. Therefore, all subgroups of a cyclic group are normal.

Problem 6.13 Prove that A_5 cannot have a normal subgroup of order 2.

Solution If A_5 has a normal subgroup say H of order 2, then H is contained in the centre of G.

Thus H has a non-identity element that commutes with every element of A_5.

Any element of A_5 of order 2 has the form $(ab)(cd)$.

But $(ab)(cd)$ does not commute with (abc), which also belong to A_5.

Therefore, A_5 cannot have a normal subgroup of order 2.

Problem 6.14 Let H be a subgroup of a group G and $N_G(H) = \{g \in G : gHg^{-1} = H\}$. We know that $N_G(H)$ is a subgroup of G. Prove that

(i) H is normal in $N_G(H)$.

(ii) If H is a normal subgroup of the subgroup K of G, then $K \subseteq N_G(H)$.

(iii) H is normal in G if and only if $N_G(H) = G$.

Solution

(i) Let $g \in N_G(H)$ and $h \in H$.

Then $gHg^{-1} = H$ and so $ghg^{-1} \in H\ \forall\ g \in N_G(H)$ and $h \in H$.

Hence H is a normal subgroup of $N_G(H)$.

(ii) Let $k \in K$.

Since H is a normal subgroup of K, therefore $kH = Hk$.

This gives $kHk^{-1} = H$ and so $k \in N_G(H)$.

Hence $K \subseteq N_G(H)$.

(iii) H is normal in $G \Leftrightarrow gHg^{-1} = H \ \forall g \in G \quad \Leftrightarrow \quad G = N_G(H)$.

Problem 6.15 Prove that A_n is a normal subgroup of S_n.

Solution We first prove that A_n is a subgroup of S_n. Since the identity permutation is an even permutation and so it belongs to A_n and hence A_n is non – empty.

Now let $f, g \in A_n$ then f, g are even permutations. Thus f, g^{-1} are even permutations and hence fg^{-1} is an even permutation and so belongs to A_n.

Therefore, A_n is a subgroup of S_n.

We now show that A_n is a normal subgroup of S_n.

Let $f \in A_n$ and $g \in S_n$, then f is even and g may be even or odd.

In case if g is even then g^{-1} is also even.

Then $g\,fg^{-1}$ is even.

Now, in case, if g is odd then g^{-1} is also odd.

Thus gfg^{-1} is even.

Therefore in both the cases we see that $gfg^{-1} \in A_n$.

Thus A_n is normal subgroup of S_n.

Problem 6.16 Prove that $SL(2, \mathbb{R})$ is a normal subgroup of $GL(2, \mathbb{R})$.

Solution We have $SL(2, \mathbb{R})$ is the group of all 2×2 matrices having determinant 1, with entries from the set $\mathbb{R}$ of real numbers.

$GL(2, \mathbb{R})$ is the group of all 2×2 matrices having non-zero determinant, with entries from the set $\mathbb{R}$ of real numbers.

Then since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2, \mathbb{R})$, so it is non empty.

Now if $A, B \in SL(2, \mathbb{R})$, then $\det(A) = \det(B) = 1$ and so $\det(AB) = 1$. Also, AB is a 2×2 matrix with real entries and hence $AB \in SL(2, \mathbb{R})$

Also for any $A \in SL(2, \mathbb{R})$, there exists a matrix A^{-1} such that $\det(A^{-1}) = 1$. So $A^{-1} \in SL(2, \mathbb{R})$.

Hence $SL(2, \mathbb{R})$ is a subgroup of $GL(2, \mathbb{R})$.

Now let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, \mathbb{R})$ be such that $\det(A) = ad - bc = 1$

and $B = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in GL(2, \mathbb{R})$ such that $xw - zy \neq 0$.

Then, $BAB^{-1} = \dfrac{1}{xw - zy}\begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} w & -y \\ -z & x \end{bmatrix}$ is a 2×2 matrix with real entries and $\det(BAB^{-1}) = (\det B)\ (\det A)\ (\det B^{-1}) = (\det B)\ (\det B^{-1}) = 1$

Thus $BAB^{-1} \in SL(2, \mathbb{R})$

and hence $SL(2, \mathbb{R})$ is a normal subgroup of $GL(2, \mathbb{R})$.

Problem 6.17 Let $H = \{(1), (12)(34)\}$ be a subgroup of A_4. Show that H is not normal in A_4.

Solution Let $h = (12)(34) \in H$ and $g = (132) \in A_4$.

Then, $ghg^{-1} = (132)(12)\ (34)(123) = (13)(24) \notin H$.

Thus, H is not a normal subgroup of A_4.

Problem 6.18 Let $H = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{R}, ad \neq 0\right\}$. Is H a normal subgroup of $GL(2, \mathbb{R})$?

Solution H is not a normal subgroup of $GL(2, \mathbb{R})$, as

let $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \in H$ and $T = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \in GL(2, \mathbb{R})$.

Then, $TAT^{-1} = \begin{bmatrix} 10 & -3 \\ 21 & -6 \end{bmatrix} \notin H$.

Therefore H is not a normal subgroup of $GL(2, \mathbb{R})$.

Problem 6.19 Show that a subgroup N of a group G is normal if and only if $xy \in N$ implies $yx \in N$.

Solution Let N be a normal subgroup of a group G.

Let $xy \in N$, where $x, y \in G$.

By definition $y(xy)y^{-1} \in N \Rightarrow yxe \in N \Rightarrow yx \in N$.

Conversely, let $xy \in N \Rightarrow yx \in N$ ...(1)

To show that N is a normal subgroup of G.

Let $g \in G$, $n \in N$ be any elements.

Then $g^{-1}(gn) \in N$ (as $g^{-1}g = e$)

Using (1), we get $(gn)g^{-1} \in N$, i.e., $gng^{-1} \in N$

Therefore, N is a normal subgroup of G.

Problem 6.20 Suppose that the group G has a subgroup of order n. Prove that, the intersection of all subgroups of G of order n, is a normal subgroup of G.

Solution Let H be a subgroup of G such that $o(H) = n$. Let $g \in G$.

Claim: gHg^{-1} is also a subgroup of G of order n.

Let $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for some $h_1, h_2 \in H$.

Then, $xy^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1})$

$= gh_1(g^{-1}g)h_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1}$

$\in gHg^{-1}$ $\quad (\because H \le G \Rightarrow h_1h_2^{-1} \in H, \forall h_1, h_2 \in H)$

Thus, $gHg^{-1} \le G$.

Also, since $o(H) = n$, we have $o(gHg^{-1}) = n$.

We now show $\bigcap_{g\in G} gHg^{-1}$ is normal in G. Let $N = \bigcap_{g\in G} gHg^{-1}$.

To show: N is a normal subgroup of G.

Since intersection of subgroups is a subgroup, therefore N is a subgroup of G.

Let $g_1 \in G$, then $g_1Ng_1^{-1} = g_1\left(\bigcap_{g\in G} gHg^{-1}\right)g_1^{-1}$

$$= \bigcap_{g\in G} g_1gHg^{-1}g_1^{-1} \in \bigcap_{g\in G} gHg^{-1} = N$$

Therefore, $g_1Ng_1^{-1} \subseteq N$. Thus, N is a normal subgroup of G.

Problem 6.21 If H is the only subgroup of finite order m in the group G, then show that H is a normal subgroup of G.

Solution Let $H = \{h_1, h_2, \ldots, h_m\}$.

For any $g \in G$, we have

$$gHg^{-1} = \{gh_1g^{-1}, gh_2g^{-1}, \ldots, gh_mg^{-1}\}$$

Then gHg^{-1} is a subgroup of G.

Further $o(gHg^{-1}) = m$, by cancellation laws in G,

as $gh_ig^{-1} = gh_jg^{-1} \Rightarrow h_i = h_j$, which is a contradiction.

Thus for each $g \in G$, gHg^{-1} is also a subgroup of G of order m.

Since H is the only subgroup of order m in G, so we must have

$$gHg^{-1} = H, \forall\ g \in G$$

Hence H is a normal subgroup of G.

Problem 6.22 Let H be a non-empty subset of a group G. Show that H is a normal subgroup of G if and only if $(gx)(gy)^{-1} \in H \ \forall \ g \in G$ and $x, y \in H$.

Solution Let H be a normal subgroup of G. Let $g \in G$ and $x, y \in H$.

Then, $(gx)(gy)^{-1} = (gx)(y^{-1}g^{-1}) = g(xy^{-1})g^{-1}$ ...(1)

Since H is a subgroup of G and $x, y \in H$, so $xy^{-1} \in H$.

Since H is a normal subgroup of G, $g(xy^{-1})g^{-1} \in H$.

Therefore from (1), we get $(gx)(gy)^{-1} \in H \ \forall g \in G$ and $x, y \in H$.

Conversely, let $(gx)(gy)^{-1} \in H \ \forall g \in G$ and $x, y \in H$. ...(2)

We shall prove that H is a normal subgroup of G.

Taking $g = e$ in (2), we get $(ex)(ey)^{-1} \in H \Rightarrow xy^{-1} \in H, \ \forall \ x, y \in H$.

Therefore H is a subgroup of G.

Now let $g \in G$ and $h \in H$. Then from (2) we have,

$$(gh)(ge)^{-1} \in H \quad \Rightarrow \quad ghe^{-1}g^{-1} \in H \ \Rightarrow \ ghg^{-1} \in H$$

Therefore, H is a normal subgroup of G.

6.2 Factor Groups

Normal subgroups are of special significance. Using the set of cosets relative to normal subgroups, new groups are constructed called the factor groups or quotient groups. When the subgroup H of a group G is normal, then the set of left (or right) cosets of H in G is itself a group, called the **factor group** of G by H or the **quotient group** of G by H.

We also study the properties of a group inherited by the factor groups. Quite often one can obtain information about a group by studying one of its factor groups.

Theorem 6.6: Let G be a group and H a normal subgroup of G. The set $G/H = \{aH : a \in G\}$ is a group under the operation $(aH)(bH) = abH$.

The group G/H is called the **factor group** of G by H or the **quotient group** of G by H.

Proof: We first show that this operation is well defined.

Let $aH = a'H$ and $bH = b'H$.

Then $a^{-1}a' \in H$ and $b^{-1}b' \in H$ and so, $a' \in aH$ and $b' \in bH$.

Thus we have, $a' = ah_1$ and $b' = bh_2$ for some $h_1, h_2 \in H$.

Therefore $a'b'H = ah_1bh_2H = ah_1bH$ $(\because \ h_2 \in H \text{ so } h_2H = H)$

$= ah_1Hb$ $(\because \ H \trianglelefteq G \text{ so } bH = Hb)$

$= aHb$ $(\because \ h_1 \in H \text{ so } h_1H = H)$

$= abH$ $(\because \ H \trianglelefteq G \text{ so } bH = Hb)$

Thus this operation is well defined.

We now show that G/H is a group under the operation $(aH)(bH) = abH$.

1. **Closure:** Let $aH, bH \in G/H$ be any two elements.

   Then $(aH)(bH) = abH \in G/H$.

2. **Associativity:**

   We have, $(aHbH)(cH) = (abH)(cH) = ((ab)c)H$

   $= a(bc)H$

   $= aH(bc)H$

   $= aH(bHcH)$

3. **Identity:** eH is the identity for G/H as

   $$aHeH = aeH = aH = eaH = eHaH, \quad \forall\, a \in G.$$

4. **Inverse:** For each $aH \in G/H$, there exists $a^{-1}H \in G/H$ such that

   $$aHa^{-1}H = (aa^{-1})H = eH = a^{-1}aH = a^{-1}HaH$$

   Thus $(aH)^{-1} = a^{-1}H, \ \forall\ a \in G.$

   Therefore, G/H is a group.

Remark: Since the center $Z(G)$ of a group G is always a normal subgroup of G, therefore, $G/Z(G)$ is a quotient group.
Also, trivial quotient groups are $G/\{e\} = G$, $G/G = \{e\}$.

Example 6.3: Let $G = \mathbb{Z}_{18} = \{0, 1, 2, \ldots, 17\} \bmod 18$ and let

$$H = \langle 6 \rangle = \{0, 6, 12\}.$$

Then, $\mathbb{Z}_{18}/H = \{H + 0, H + 1, H + 2, H + 3, H + 4, H + 5\}$. .

Example 6.4: Let $G = (\mathbb{Z}, +)$ and $N = \langle 4 \rangle = \{0, \pm 4, \pm 8, \pm 12, \ldots\}$.

Then, $\mathbb{Z}/N = \{N + 0, N + 1, N + 2, N + 3\}$.

Problem 6.23 If G is a finite group and N is a normal subgroup of G, then

$$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}$$

Solution Since G is finite, therefore by Lagrange's theorem

$\dfrac{o(G)}{o(N)}$ = number of distinct left (right) cosets of N in $G = o\left(\dfrac{G}{N}\right)$.

Problem 6.24 Prove that the factor group of an abelian group is abelian.

Solution Let G be an abelian group and let G/N be any factor group of G.

Then for any $Na, Nb \in G/N$, we have

$$\begin{aligned}(Na)(Nb) &= N(ab)\\ &= N(ba) \qquad (\because\ G \text{ is Abelian})\\ &= (Nb)(Na)\end{aligned}$$

Thus G/N is Abelian.

However, the converse is not true. Consider the following example.

Example 6.5: Consider $S_3 = \{I, (12), (13), (23), (123), (132)\}$

Let A_3 be the alternating group, then $A_3 = \{I, (123), (132)\}$.

Also, A_3 is a normal subgroup of S_3 and $o\left(\frac{S_3}{A_3}\right) = \frac{o(S_3)}{o(A_3)} = \frac{6}{3} = 2.$

Since, every group of prime order is cyclic and every cyclic group is abelian, therefore S_3/A_3 is abelian but S_3 is non-abelian.

Problem 6.25 Prove that the factor group of a cyclic group is cyclic.

Solution Let $G = \langle a \rangle$ be any cyclic group and let G/N be any factor group of G.

To show that G/N is cyclic, we will show that $G/N = \langle aN \rangle$.

Let $xN \in G/N$ be any element.

Now $x \in G = \langle a \rangle$, so $x = a^m$ for some $m \in \mathbb{Z}$.

Then $xN = a^m N = a \cdot a \cdot \ldots aN$ (m times)

$= (aN)(aN) \ldots (aN)$ (m times)

$= (aN)^m$.

Thus $G/N = \langle aN \rangle$ and hence G/N is cyclic.

However the converse may not be true. Consider the following example.

Example 6.6: Let $G = S_3$, then A_3 is a normal subgroup of S_3. Since S_3 is non-abelian, S_3 cannot be cyclic. But $o\left(\frac{S_3}{A_3}\right) = \frac{o(S_3)}{o(A_3)} = \frac{6}{3} = 2,$ therefore S_3/A_3, being of prime order, is cyclic.

Problem 6.26 If N is a normal subgroup of a group G and $a \in G$ is of order $o(a)$, prove that $o(Na)$ divides $o(a)$. Also show that $a^m \in N$ if and only if $o(Na)$ divides m.

Solution Let $o(a) = n$, so that n is the least positive integer such that

$$a^n = e \qquad \ldots(1)$$

Consider $(Na)^n = Na \cdot Na \ldots Na$ (n times)

$$= Na.a...a \ (n \text{ times}) = Na^n = Ne = N$$

Therefore $(Na)^n = N$, identity of G/N.

Hence $o(Na)$ divides $o(a)$.

Now $a^m \in N \Leftrightarrow Na^m = N \Leftrightarrow (Na)^m = N$ (as N is a normal subgroup of G)

$$\Leftrightarrow \ o(Na) \text{ divides } m.$$

Problem 6.27 Let N be a normal subgroup of G. Show that every subgroup of G/N is of the form H/N, where H is any subgroup of G.

Solution Let K be any subgroup of G/N and let $H = \{x \in G : xN \in K\}$.

We will show that $H/N = K$.

Let $x \in N$, then $xN = N = eN$ = identity of $G/N \in K$

Thus, $xN \in K$ gives that $x \in H$ and so $N \subseteq H$.

We now show that H is a subgroup of G. Let $h_1, h_2 \in H$, then $h_1N, h_2N \in K$.

Since $K \leq G/N$, $(h_1N)(h_2N)^{-1} \in K$. Then, $(h_1N)(h_2^{-1}N) \in K$ and so

$$h_1h_2^{-1}N \in K.$$

Thus $h_1h_2^{-1} \in H$ and so H is a subgroup of G.

Hence H is a subgroup of G containing N.

Let $x \in N$, $h \in H \subseteq G$ and N is normal subgroup of G, so $h^{-1}xh \in N$. Hence N is normal in H. Thus H/N is defined.

Now let $hN \in H/N$. Then $h \in H$ and so $hN \in K$. Thus $H/N \subseteq K$.

Otherway, let $xN \in K$, then $x \in H$. So $xN \in H/N$ and hence $K \subseteq H/N$.

Therefore $K = H/N$ and so any subgroup of G/N is of the form H/N.

Problem 6.28 If H is a normal subgroup of a group G and G is finite, then show that G/H is finite. But the converse may not hold.

Solution Let G be finite.

Then, G has only finite number of distinct right cosets of H in G, i.e., $i_G(H)$ is finite.

Hence $o\left(\dfrac{G}{H}\right) = i_G(H)$ is finite.

But the converse need not hold, i.e., G/H is finite but G may not be finite.

Let $G = (\mathbb{Z}, +)$ then G is of infinite order.

Let $H = \{3x : x \in \mathbb{Z}\}$. Then H is a normal subgroup of G

Also, $\frac{G}{H} = \{H, H + 1, H + 2\}$ is finite.

Therefore $(\mathbb{Z}, +)$ is infinite but $\mathbb{Z}/H$ is finite.

Remark: From the above example we note that if $Ha = Hb$, then a may not be equal to b as $H + 4 = H + 1$ but $4 \neq 1$.

Problem 6.29 Find the order of

(a) $5 + \langle 6\rangle$ in $\frac{\mathbb{Z}_{18}}{\langle 6\rangle}$

(b) $14 + \langle 8\rangle$ in $\frac{\mathbb{Z}_{24}}{\langle 8\rangle}$

Solution

(a) Let $G = \mathbb{Z}_{18}$ and $H = \langle 6\rangle = \{0, 6, 12\}$.

Since $6 \in \mathbb{Z}_{18}$ is of order 3, therefore $o(H) = 3$.

Then $o\left(\frac{G}{H}\right) = \frac{18}{3} = 6.$

The possible orders of the elements of G/H are divisors of 6, that is 1,2,3 or 6.

Now $5 + \langle 6\rangle = 5 + H \in \frac{G}{H}$ and $2(5 + H) = 10 + H = 4 + H$, as H absorbs multiples of 6,

Also $3(5 + H) = 3 + H$, $6(5 + H) = H$. Hence order of $5 + H$ is 6.

(b) Let $G = \mathbb{Z}_{24}$ and $H = \langle 8\rangle = \{0, 8, 16\}$

Since $8 \in \mathbb{Z}_{24}$ is of order 3, therefore $o(H) = 3$.

Then $o\left(\frac{G}{H}\right) = \frac{24}{3} = 8.$

The possible orders of the elements of G/H are divisors of 8, that is 1,2,4 or 8.

Now $14 + \langle 8\rangle = 14 + H = 6 + H$ and $2(6 + H) = 4 + H$, $3(6 + H) = 2 + H$, $4(6 + H) = H$ as H absorbs multiples of 6.

Hence order of $14 + H$ is 4.

Problem 6.30 Let N be a normal subgroup of a group G and let H be a subgroup of G. If N is a subgroup of H, prove that H/N is a normal subgroup of G/N if and only if H is a normal subgroup of G.

Solution Let H be a normal subgroup of G.

To show that H/N is a normal subgroup of G/N.

Let $Ng \in G/N$ and $Nh \in H/N$ be any elements. Then $g \in G$ and $h \in H$.

Since H is a normal subgroup of G, so $g^{-1}hg \in H$.

Now $(Ng)^{-1}\, Nh(Ng) = Ng^{-1}NhNg = Ng^{-1}hg$ $(\because\ N \trianglelefteq G)$

$\in H/N$ as $g^{-1}hg \in H$.

Thus, H/N is normal in G/N.

Conversely, let H/N be a normal subgroup of G/N.

To show that H is a normal subgroup of G.

Let $h \in H$ and $g \in G$ be any elements. Then $Nh \in H/N$ and $Ng \in G/N$.

Since H/N is normal in G/N we have $(Ng)^{-1}Nh(Ng) \in H/N$

$\Rightarrow$ $Ng^{-1}NhNg \in H/N$

$\Rightarrow$ $Ng^{-1}hg \in H/N$ $(\because\ N \trianglelefteq G)$

Then $Ng^{-1}\, hg = Nh_1$ for some $h_1 \in H$.

$\Rightarrow$ $g^{-1}hgh_1^{-1} \in N \subseteq H$ $(\because\ Ha = Hb \Rightarrow ab^{-1} \in H)$

Thus $g^{-1}hg \in H$ and hence H is a normal subgroup of G.

Problem 6.31 If N is a normal subgroup of a group G and $o(G/N) = m$, then show that $x^m \in N$, $\forall x \in G$.

Solution Let $x \in G$ be any element. Then, $Nx \in G/N$.

Therefore $(Nx)^{o(G/N)} = N$ $(\because\ a^{o(G)} = e)$

$\Rightarrow$ $(Nx)^m = N$

$\Rightarrow$ $\underbrace{(Nx)(Nx)...(Nx)}_{m \text{ times}} = N$

$\Rightarrow$ $N\underbrace{(xx\ ...\ x)}_{m \text{ times}} = N$, as N is a normal subgroup of G

$\Rightarrow$ $Nx^m = N$

Thus $x^m \in N$.

Problem 6.32 Let H be a normal subgroup of a finite group G. If $\gcd(o(x), o(G/H)) = 1$, show that $x \in H$.

Solution Let $x \in G$, then $Hx \in G/H$. Then $o(Hx) \mid o(G/H)$.

Let $o(x) = n$ then $x^n = e$.

Now $(Hx)^n = (Hx)(Hx) \ldots (Hx) = H(xx \ldots x)$ $(\because H \trianglelefteq G)$

$= Hx^n = He = H.$

Since $(Hx)^n = H$, therefore $o(Hx) \mid n = o(x)$.

Thus $o(Hx) \mid o(x)$. Also $o(Hx) \mid o(G/H)$

But $\gcd(o(x), o(G/H)) = 1$, therefore $o(Hx) = 1$.

Thus $Hx = H$ and so $x \in H$.

Problem 6.33 Prove that A_4 has no subgroup of order 6.

Solution Suppose A_4 has a subgroup H of order 6.

Then $i_{A_4}(H) = \dfrac{o(A_4)}{o(H)} = 2$. Hence H is normal in A_4

Therefore A_4/H exists and $o\left(\dfrac{A_4}{H}\right) = \dfrac{o(A_4)}{o(H)} = 2$.

Now let $H\alpha \in A_4/H$ be any arbitrary element. Then $(H\alpha)^2 = H$

So $(H\alpha)(H\alpha) = H \Rightarrow H\alpha^2 = H \Rightarrow \alpha^2 \in H, \quad \forall \alpha \in A_4$

Thus $H = \{I$, eight 3 cycles$\}$ as $(abc)^2$ is a 3 cycle.

Hence $o(H) = 9$, which is not true as $o(H) = 6$.

Therefore A_4 does not have a subgroup of order 6.

Problem 6.34 Let $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where

$i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$ $ki = j = -ik$.

(a) Show that $H = \{1, -1\}$ is a normal subgroup of G.

(b) Construct the Cayley table for G/H.

Solution

(a) We have $H = \{1, -1\}$. Then since H is center of G, so H is normal in G.

(b) The cosets of H in G are $1H$, $-1H$, $\pm iH$, $\pm jh$, $\pm kH$.

Table 6.1: The Cayley Table of *G/H*

	$1H$	$-1H$	iH	$-iH$	jH	$-jH$	kH	$-kH$
$1H$	H	$-1H$	iH	$-iH$	jH	$-jH$	kH	$-kH$
$-1H$	$-1H$	$1H$	$-iH$	iH	$-jH$	jH	$-kH$	kH
iH	iH	$-iH$	$-1H$	$1H$	kH	$-kH$	$-jH$	jH
$-iH$	$-iH$	iH	$1H$	$-1H$	$-kH$	kH	jH	$-jH$
jH	jH	$-jH$	$-kH$	kH	$-1H$	$1H$	iH	$-iH$
$-jH$	$-jH$	jH	kH	$-kH$	$1H$	$-1H$	$-iH$	iH
kH	kH	$-kH$	jH	$-jH$	$-iH$	iH	$-1H$	$1H$
$-kH$	$-kH$	kH	$-jH$	jH	iH	$-iH$	$1H$	$-1H$

Problem 6.35 Let N be a normal subgroup of a group G. Show that G/N is abelian if and only if $xyx^{-1}y^{-1} \in N$ for all $x, y \in G$.

Solution G/N is abelian $\Leftrightarrow NxNy = NyNx$ for all $x, y \in G$

$\Leftrightarrow \quad Nxy = Nyx$ for all $x, y \in G$

$\Leftrightarrow \quad (xy)(yx)^{-1} \in N$ for all $x, y \in G$

$\Leftrightarrow \quad xyx^{-1}y^{-1} \in N$ for all $x, y \in G$.

6.3 Commutator Subgroup of a Group and its Properties

Definition 6.4: Generators for a Subgroup:

Let S be a non-empty subset of a group G. Let

$$H = \{x_1x_2 \ldots x_k : k \text{ is finite but not fixed, } x_i \text{ or } x_i^{-1} \in S \text{ for all } i\}$$

We claim that H is a subgroup of G containing S.

Since $S \neq \phi$ therefore $H \neq \phi$.

Now let $x, y \in H$ then $x = x_1x_2 \ldots x_n, \quad x_i$ or $x_i^{-1} \in S$

and $\quad y = y_1y_2 \ldots y_m, \quad y_j$ or $y_j^{-1} \in S$

Then $xy^{-1} = x_1x_2 \ldots x_n{y_m}^{-1} \ldots {y_2}^{-1}{y_1}^{-1} \in H$ (by definition of H).

Therefore H is a subgroup of G.

Also by definition of H, we have that $S \subseteq H$.

We now show that H is the smallest subgroup of G containing S.

Let K be any other subgroup of G containing S and let $h \in H$ be any element.

Then $h = x_1x_2 \ldots x_n$, x_i or $x_i^{-1} \in S$.

Now if $x_i \in S$ then $x_i \in K$. And, if $x_i^{-1} \in S$, then $x_i^{-1} \in K$, so $x_i \in K$.

Therefore $h \in K$ and hence $H \subseteq K$.

Thus H is the smallest subgroup of G containing S.

We say that ***H* is a subgroup generated by *S*** and write $H = \langle S \rangle$.

Definition 6.5: Let G be a group and let $a, b \in G$. Elements of the type $a^{-1}b^{-1}ab$ are called **commutators in *G***.

Definition 6.6: Let S denotes the set of all commutators in G and let G' denote the subgroup of G generated by S, then ***G′* is called commutator subgroup of *G*.**

Since G' is a subgroup generated by S, therefore $x \in G'$ gives

$$x = c_1c_2 \ldots c_n, \text{ where } c_i \in S \text{ or } c_i^{-1} \in S.$$

Problem 6.36 Let G be a group and let G' be the subgroup of G generated by the set $S = \{x^{-1}y^{-1}xy : x, y \in G\}$.

(a) Prove that G' is normal in G.

(b) Prove that G/G' is abelian.

(c) If G/N is abelian then prove that $G' \subseteq N$.

(d) Prove that if H is a subgroup of G and $G' \subseteq H$, then H is a normal subgroup of G.

Solution

(a) Let $g \in G$ and $x \in G'$. Then, $x = c_1c_2 \ldots c_n$, where $c_i \in S$ or $c_i^{-1} \in S$.

Now, $c_i \in S$ means that c_i is a commutator. Thus, $c_i = a_i^{-1}b_i^{-1}a_ib_i$ for some $a_i, b_i \in G$.

Also $c_i^{-1} \in S$ implies c_i^{-1} is a commutator. So, $c_i^{-1} = \alpha_i^{-1}\beta_i^{-1}\alpha_i\beta_i$.

Thus $c_i = \beta_i^{-1}\alpha_i^{-1}\beta_i\alpha_i$ and hence c_i is a commutator.

Therefore for each i, c_i is a commutator.

Now $g^{-1}xg = g^{-1}(c_1c_2 \ldots c_n)g = (g^{-1}c_1g)(g^{-1}c_2g) \ldots (g^{-1}c_ng)$

But $g^{-1}c_ig = g^{-1}(a_i^{-1}b_i^{-1}a_ib_i)g = (g^{-1}a_ig)^{-1}(g^{-1}b_ig)^{-1}(g^{-1}a_ig)(g^{-1}b_ig)$

$= \alpha_i^{-1}\ \beta_i^{-1}\ \alpha_i\beta_i$

where $\alpha_i = g^{-1}a_ig$ and $\beta_i = g^{-1}b_ig$.

Therefore $g^{-1}c_ig \in S$ for all i. Hence $g^{-1}xg \in G'$.

So G' is normal subgroup of G.

(b) Consider $G'xG'y$.

We have, $G'xG'y = G'yG'x$.

$\Leftrightarrow$ $G'xy = G'yx$. ($\because$ G' is a normal subgroup of G)

$\Leftrightarrow$ $(xy)(yx)^{-1} \in G'$ ($\because$ $Ha = Hb \Leftrightarrow ab^{-1} \in H$)

$\Leftrightarrow$ $xyx^{-1}y^{-1} \in G'$

which is true, as G' contains all commutators of G.

Hence G/G' is abelian.

(c) Since G/N is abelian, we have $Nx\,Ny = NyNx\ \forall\ x, y \in G$

$\Rightarrow$ $Nxy = Nyx$ ($\because$ $N \trianglelefteq G$)

$\Rightarrow$ $(xy)(yx)^{-1} \in N$ (as $Ha = Hb \Leftrightarrow ab^{-1} \in H$)

$\Rightarrow$ $xyx^{-1}y^{-1} \in N, \forall\ x, y \in G$.

$\Rightarrow$ $S \subseteq N$ ($\because$ S is the set of all commutators $xyx^{-1}y^{-1}$).

But G' is the smallest subgroup of G containing S, therefore $G' \subseteq N$.

(d) Let $h \in H$ and $g \in G$.

Then $ghg^{-1}h^{-1} \in G' \subseteq H$. This gives $ghg^{-1} \in Hh = H$.

Thus H is a normal subgroup of G.

6.4 The G/Z Theorem

The next theorem illustrates how knowledge of a factor group of a group G divulges information about G.

Theorem 6.7: If for a group G, $G/Z(G)$ is cyclic, then G is abelian.

Proof: Let us write $N = Z(G)$, then G/N is cyclic.

Let $G/N = \langle Ng \rangle$ for some $Ng \in G/N$

Let $a, b \in G$ be any elements. Then $Na, Nb \in G/N = \langle Ng \rangle$.

$\Rightarrow$ $Na = (Ng)^m$ and $Nb = (Ng)^n$ for some $m, n \in \mathbb{Z}$.

$\Rightarrow$ $Na = Ng^m$ and $Nb = Ng^n$ ($\because$ $N \trianglelefteq G$)

$\Rightarrow$ $ag^{-m} \in N$ and $bg^{-n} \in N$ ($\because$ $Ha = Hb \Leftrightarrow ab^{-1} \in H$)

$\Rightarrow$ $ag^{-m} = x$ and $bg^{-n} = y$ for some $x, y \in N$.

$\Rightarrow$ $a = xg^m$ and $b = yg^n$.

Thus $ab = xg^m yg^n = xyg^m g^n$ (as $y \in N = Z(G)$)

$= xyg^{m+n}$

And, $ba = yg^n xg^m = yxg^n g^m$ (as $x \in N = Z(G)$)

$= xyg^{m+n}$ (as $y \in N = Z(G)$ and $x \in G$)

Hence $ab = ba$. Therefore G is abelian.

Remark: If G/H is a cyclic group, it may not mean G is abelian.

EXAMPLE 6.5: Let $G = Q_8$ (Quaternion Group), and let $H = \{\pm 1, \pm i\}$. Then $H \trianglelefteq G$.

Also $o\left(\frac{G}{H}\right) = \frac{o(G)}{o(H)} = \frac{8}{4} = 2$, which is a prime.

Therefore G/H is cyclic, but G is not abelian.

However if G/H is a cyclic group and H is a subgroup of $Z(G)$, then G is abelian.

Remark: It is the contrapositive statement of the G/Z Theorem that is most often used which states that: If G is non-abelian, then $G/Z(G)$ is non-cyclic.

PROBLEM 6.37 If G is a non-abelian group of order pq where p, q are primes, then prove that $o(Z(G)) = 1$, i.e., if G is non-abelian group of order pq, then it has a trivial centre.

SOLUTION Since $Z(G) \leq G$, so by Lagrange's theorem $o(Z(G)) \mid o(G) = pq$

Thus $o(Z(G)) = 1, p, q, pq$.

If $o(Z(G)) = pq$, then $Z(G) = G$.

Since $Z(G)$ is abelian, so G is abelian, which is not true.

Hence $o(Z(G)) \neq pq$.

If $o(Z(G)) = q$, then $o\left(\frac{G}{Z(G)}\right) = \frac{pq}{q} = p = \text{prime}$.

Since group of prime order is cyclic, therefore, $\frac{G}{Z(G)}$ is cyclic and hence G is abelian, by G/Z Theorem, which is a contradiction.

Hence $o(Z(G)) \neq q$. Similarly $o(Z(G)) \neq p$.

Thus $o(Z(G)) = 1$.

PROBLEM 6.38 If G is a non-abelian group of order p^3 (where p is prime) and $Z(G) \neq \{e\}$, then prove that $o(Z(G)) = p$.

SOLUTION Since $Z(G)$ is a subgroup of G, so by Lagrange's theorem $o(Z(G)) \mid o(G) = p^3$

Thus $o(Z(G)) = 1, p, p^2$ or p^3.

If $o(Z(G)) = p^3$, then $Z(G) = G$.

Since $Z(G)$ is abelian, so, G is abelian, which is not true. Hence $o(Z(G)) \neq p^3$.

If $o(Z(G)) = p^2$, then $o\left(\frac{G}{Z(G)}\right) = \frac{p^3}{p^2} = p = \text{prime}$.

Since a group of prime order is cyclic, therefore $\frac{G}{Z(G)}$ is cyclic and hence G is abelian, a contradiction.

Therefore $o(Z(G)) \neq p^2$

Thus $o(Z(G)) = 1$ or p. Since $Z(G) \neq \{e\}$, hence $o(Z(G)) = p$.

6.5 Cauchy's Theorem for Abelian Group

In the next theorem, we discuss the existence of elements of all possible prime orders in a finite group. It demonstrates one of the most dominant techniques available in the theory of finite groups. It can be viewed as a partial converse to Lagrange's theorem,

Theorem 6.8: Let G be a finite Abelian group and let p be a prime such that $p \mid o(G)$. Then G has an element of order p, i.e., there exists some $x \in G$ such that $o(x) = p$.

Proof: We shall prove the theorem by induction on $n = o(G)$.

Since G is abelian if and only if $x^2 = e$, $\forall\, x \in G$, so the result is true for $n = 2$.

We assume the result to be true for all abelian groups having order less than $o(G)$.

We shall prove that it is also true for $o(G)$.

If G has no non-trivial subgroups, then G must be of prime order because every group of composite order possesses non-trivial subgroups. But p is prime and $p \mid o(G)$, therefore, $o(G) = p$. Also every group of prime order is cyclic,

Therefore $G = \langle x \rangle$ such that $o(x) = o(G) = p$. So the result follows.

We now assume that G has non-trivial subgroups.

Let H be a subgroup of G such that $H \neq \{e\}$, G.

If $p \mid o(H)$, then by induction hypothesis the theorem is true for H because H is an abelian group and $o(H)$ is less than $o(G)$.

Therefore there exists an element $x \in H$, such that $o(x) = p$.

Also $x \in H$ implies $x \in G$. So result is again true.

Now if $p \nmid o(H)$, then since every subgroup of an abelian group is normal, therefore H is a normal subgroup of G.

Since $o(G) = o(G/H) \cdot o(H)$ and $p \mid o(G)$, we find $p \mid o(G/H) \cdot o(H)$.

But $p \nmid o(H)$, hence $p \mid o(G/H)$. Also, $o(G/H) < o(G)$ as $o(H) > 1$ and G is abelian means G/H is abelian. So, by induction hypothesis, G/H has an element Hy of order p.

Thus, $(Hy)^p = H$

$\Rightarrow$ $Hy^p = H$

$\Rightarrow$ $y^p \in H$.

$\Rightarrow$ $(y^p)^t = e$ where $t = o(H)$.

$\Rightarrow$ $(y^t)^p = e$

$\Rightarrow$ $o(y^t) \mid p$.

Thus $o(y^t) = 1$ or p

If $o(y^t) = 1$ then $y^t = e$, and so, $Hy^t = He = H$. Thus $(Hy)^t = H$

Therefore $o(Hy) | t \Rightarrow p | t = o(H)$, a contradiction.

Thus $o(y^t) = p$, $y^t \in G$.

So the result is true in this case also.

Thus by induction, result is true for all abelian groups.

Corollary 6.1: Let G be an Abelian group of finite order. If p is a prime number which divides $o(G)$, then G has a subgroup of order p.

Proof: By the above theorem, G has an element x of order p.

Then $H = \langle x \rangle$ is the required subgroup of order p.

Remark: By virtue of the above corollary, we observe that a partial converse of Lagrange's theorem holds, when p divides $o(G)$, p being a prime number.

As a consequence of this, a group of order 12 must have subgroups of orders 2 and 3, since 2 and 3 are prime numbers which divide $o(G) = 12$.

However we cannot say whether the group will have a subgroup of order 4 or 6.

Problem 6.39 Give an example of an infinite group in which each element has finite order.

Solution Consider the factor group $\mathbb{Q}/\mathbb{Z}$, where $\mathbb{Q}$ is the set of rationals and $\mathbb{Z}$ is the set of integers.

Then, $$\frac{\mathbb{Q}}{\mathbb{Z}} = \left\{ \frac{m}{n} + \mathbb{Z} : \frac{m}{n} \in \mathbb{Q} \right\}.$$

Let $\frac{m}{n} + \mathbb{Z} \in \frac{\mathbb{Q}}{\mathbb{Z}}$ be any element, then

$$n\left(\frac{m}{n} + \mathbb{Z}\right) = n\left(\frac{m}{n}\right) + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z} \quad (\because H + a = H \Leftrightarrow a \in H)$$

$\Rightarrow$ $o\left(\frac{m}{n} + \mathbb{Z}\right) \leq n$, i.e., finite.

Now we show that $\mathbb{Q}/\mathbb{Z}$ has infinite order.

Let $o\left(\frac{\mathbb{Q}}{\mathbb{Z}}\right) = n$ = finite. Let $x + \mathbb{Z} \in \frac{\mathbb{Q}}{\mathbb{Z}}$ be any element.

Then $n(x + \mathbb{Z}) = \mathbb{Z}$ ($\because$ if $a \in G$, $a^{o(G)} = e$)

So $nx + \mathbb{Z} = \mathbb{Z}$ and therefore $nx \in \mathbb{Z}$. This is true $\forall\ x \in \mathbb{Q}$

In particular, for $x = \frac{1}{3n}$, we have $n\cdot\frac{1}{3n} \in \mathbb{Z}$ implies $\frac{1}{3} \in \mathbb{Z}$, which is a contradiction.

Therefore $\frac{\mathbb{Q}}{\mathbb{Z}}$ is of infinite order.

Exercises

1. Let $H = \{(1), (12)\}$. Is H normal in S_3?
2. If $o(G) = pq$, where p, q are not necessarily distinct primes then show that $o(Z(G)) = 1$ or pq.
3. Let $G = D_4$ and $H = \{R_0, R_{90}, R_{180}, R_{270}\}$. Show that H is a normal subgroup of D_4.
4. Let $G = D_4$ and $H = \{R_0, R_{180}\}$. Find the factor group G/H.
5. Let G be a group such that $o(G) = 15$ and $\mathbb{Z}(G) \neq \{e\}$, show that G is abelian.
6. Construct Cayley table for $U(30)/U_5(30)$.
7. Find the order of $12 + \langle 8\rangle$ in $Z_{24}/\langle 8\rangle$.
8. Find the commutator subgroup of S_3.
9. Prove that if G is finite then G/N is finite, but converse may not hold.
10. Let $G = \mathbb{Z}$ and $H = 6\mathbb{Z}$. Find the factor group G/H.
11. Let a be an element of a group G such that $o(a)$ is finite. If H is a normal subgroup of G, then prove that $o(aH)$ divides $o(a)$.
12. Let N be a normal cyclic subgroup of a group G. If H is a subgroup of N, then prove that H is a normal subgroup of G.

Hints to Selected Problems

1. No.

$\because$ $(12)(123) \neq (123)(12)$ for $(123) \in S_3$ and $(12) \in H$.

11. Let $O(a) = n$. Then, $(aH)^n = a^nH = eH = H$. Thus, $O(aH)$ divides n.

12. Since N is cyclic, $N = \langle a\rangle$ for some $a \in N$. Since H is a subgroup of N and every subgroup of a cyclic group is cyclic and $N = \langle a\rangle$, we have $H = \langle a^m\rangle$ for some integer m. Let $g \in G$, and let $b \in H = \langle a^m\rangle$.

Then, $b = a^{mk}$ for some integer k. Since $N = \langle a\rangle$ is normal in G,

We have, $g^{-1}ag = a^n \in N$ for some integer n.

Therefore, $g^{-1}bg = g^{-1}a^{mk}\ g = (g^{-1}ag)^{mk} = (a^n)^{mk} = a^{mkn} \in H = \langle a^m\rangle$.

Check for updates

7

Group Homomorphism and Isomorphism

Learning Objectives

- Homomorphism of Groups and its Properties
- Properties of Subgroups under Homomorphism
- Isomorphism of Groups
- Theorems Based on Isomorphism of Groups and its Properties

7.1 Homomorphism of Groups and its Properties

We introduce the notion of homomorphism† of groups as a map between two groups which respects the group structure so that we may establish relationship between various groups. These mappings are of great interest and importance. In fact they are as essential to group theory as continuous functions are to topology. Etymologically the word homomorphism can be traced to the Greek roots "homo" and "morph" together mean "same shape".

Definition 7.1: Let $(G, *)$ and $(G', \circ)$ be two groups. A mapping $f : G \to G'$ is called a **group homomorphism** if

$$f(a * b) = f(a) \circ f(b), \ \forall \ a, b \in G$$

In other words, a homomorphism is a map from one group to another that preserves the group operation.

To avoid confusion, we shall use the same symbol for both the binary compositions.

† The concept of homomorphism of groups was introduced by Camille Jordan in 1870, in his book "Traité des Substitutions".

© The Author(s) 2023

D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_7

With that as notation, we say that a map $f : G \to G'$ is a homomorphism, if

$$f(ab) = f(a)f(b), \forall\ a, b \in G.$$

If $f : G \to G'$ is onto homomorphism, then G' is called **homomorphic image of *G*.**

We define kernel of a homomorphism and study properties of homomorphism.

Definition 7.2: Let $f : G \to G'$ be a homomorphism, then the set

$$\{x \in G : f(x) = e',\ e' \text{ being identity of } G'\}$$

is called **kernel of homomorphism *f***, denoted by *kerf*.

Before giving some properties about homomorphisms, we present some examples.

Examples on Homomorphism

1. Define $\varphi : \mathbb{Z} \to \mathbb{Z}$ such that $\varphi(x) = 3x, \forall x \in \mathbb{Z}$.

   Then $\varphi(a + b) = 3(a + b) = 3a + 3b = \varphi(a) + \varphi(b)$

   Thus φ is a homomorphism and

   $$\begin{aligned}\ker \varphi &= \{x \in \mathbb{Z} : \varphi(x) = 0\}\\ &= \{x \in \mathbb{Z} : 3x = 0\}\\ &= \{x \in \mathbb{Z} : x = 0\}\\ &= \{0\}\end{aligned}$$

2. Let $G = GL(2, \mathbb{R})$ and let $\mathbb{R}^*$ be the group of non-zero real numbers under multiplication.

   Define $\varphi : G \to \mathbb{R}^*$ such that $\varphi(A) = \det A$ $\qquad (\det A \in \mathbb{R}^*)$

   To verify that φ is homomorphism.

   We have $\varphi(AB) = \det(AB) = \det A \cdot \det B = \varphi(A) \cdot \varphi(B)$

   Thus φ is homomorphism.

   Now we have $\quad \ker\varphi = \{x \in G : \varphi(x) = e'\}.$

   $$\begin{aligned}&= \{A \in G : \varphi(A) = 1\}\\ &= \{A \in G : \det A = 1\}\\ &= SL(2, \mathbb{R})\end{aligned}$$

3. Define $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ such that $\varphi(x) = |x|, \forall x \in \mathbb{R}^*$

   Then $\quad \varphi(xy) = |xy| = |x|\,|y| = \varphi(x)\ \varphi(y).$

   Therefore φ is a homomorphism.

   And $\ker \varphi = \{x \in \mathbb{R}^* : \varphi(x) = 1\}$

   $$= \{x \in \mathbb{R}^* : |x| = 1\} = \{1, -1\}$$

4. Let $R[x]$ denote the group of all polynomials with real coefficients under addition.

   Define $\varphi : R[x] \to R[x]$ such that $\varphi(P(x)) = P'(x)$.

   Now $\varphi(P(x) + Q(x)) = (P(x) + Q(x))' = P'(x) + Q'(x)$
   $= \varphi(P(x)) + \varphi(Q(x))$.

   Thus φ is homomorphism.

   Also $\ker \varphi = \{P(x) \in R[x] : \varphi(P(x)) = 0\}$
   $= \{P(x) \in R[x] : P'(x) = 0\}$
   $=$ set of all constant polynomials.

5. Define $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ such that $\varphi(m) = r$, where r is the remainder, when m is divided by n.

   Then φ is homomorphism as

   $\varphi(a + b) = r_{a+b}$, the remainder when $a + b$ is divided by n
   $= r_a + r_b$, the remainder when a is divided by n + the remainder when b is divided by n
   $= \varphi(a) + \varphi(b)$

   Also $\ker \varphi = \{m \in \mathbb{Z} : \varphi(m) = 0\} = \{m \in \mathbb{Z} : r = 0\}$
   $= \{m \in \mathbb{Z} : m = nk \text{ for some } k \in \mathbb{Z}\}$
   $= \langle n \rangle$.

   For example, if $\varphi : \mathbb{Z} \to \mathbb{Z}_5$ and $a = 7$, $b = 6$.

   Then $a + b = 7 + 6 = 13$, $\varphi(a + b) = \varphi(13) = 3$

   Also $\varphi(a) \oplus_5 \varphi(b) = \varphi(7) \oplus_5 \varphi(6) = 2 \oplus_5 1 = 3$

   Thus $\varphi(a + b) = \varphi(a) \oplus_5 \varphi(b)$.

Problem 7.1 Prove that the mapping $x \to x^6$ from $\mathbb{C}^*$ to $\mathbb{C}^*$ is a homomorphism. What is the kernel?

Solution Let $x, y \in \mathbb{C}^*$.

Then $f(xy) = (xy)^6 = x^6y^6 = f(x)f(y)$ (As $\mathbb{C}^*$ is Abelian)

Therefore f is homomorphism.

Now let $x \in \ker f$, then $f(x) = 1$ implying $x^6 = 1$.

Therefore $\ker f = \{x \in \mathbb{C}^* : f(x) = 1\}$
$= \{x \in \mathbb{C}^* : x^6 = 1\}$
$= \{x \in \mathbb{C}^* : x = (\cos 2k\pi + i \sin 2k\pi)^{1/6}\}$

$$= \left\{ x \in \mathbb{C}^* : x = \cos\frac{2k\pi}{6} + i \sin\frac{2k\pi}{6}, k = 0,1,\ldots 5 \right\}$$

$$= \left\{ x \in \mathbb{C}^* : x = \cos\frac{k\pi}{3} + i \sin\frac{k\pi}{3}, k = 0,1,\ldots 5 \right\}$$

Properties of Homomorphism

Theorem 7.1: Let φ be a homomorphism from a group G to a group G' and let g be an element of G. Then

1. φ carries identity of G to identity of G'.
2. $\varphi(g^n) = (\varphi(g))^n$, $n \in \mathbb{Z}$
3. If $o(g) = n$, then $o(\varphi(g))$ divides n.
4. If $\varphi(g) = g'$ then $\varphi^{-1}(g') = \{x \in G : \varphi(x) = g'\} = g \ker \varphi$

Proof:

1. To show that $\varphi(e) = e'$

   Consider $\varphi(e) = \varphi(ee) = \varphi(e)\,\varphi(e)$ ($\because$ φ is homomorphism)

   $\Rightarrow \varphi(e) \cdot e' = \varphi(e)\,\varphi(e)$

   $\Rightarrow e' = \varphi(e)$ (By left cancellation law)

2. If $n = 0$, then to show that $\varphi(g^0) = \{\varphi(g)\}^0$, we need to show $\varphi(e) = e'$, which is true.

   If $n \in \mathbb{Z}_+$, then we proceed by induction.

   For $n = 1$, LHS = RHS = $\varphi(g)$.

   Assume that $\varphi(g^n) = \{\varphi(g)\}^n$

   To show that $\varphi(g^{n+1}) = \{\varphi(g)\}^{n+1}$

   Now $\varphi(g^{n+1}) = \varphi(g^n \cdot g) = \varphi(g^n) \cdot \varphi(g)$ ($\because$ φ is homomorphism)

   $= \{\varphi(g)\}^n \cdot \varphi(g) = \{\varphi(g)\}^{n+1}$ (by induction hypothesis)

   If n is negative, then $-n$ is positive.

   Then $e' = \varphi(e) = \varphi(g^n \cdot g^{-n}) = \varphi(g^n) \cdot \varphi(g^{-n})$

   Now $\varphi(g^{-n}) = \{\varphi(g)\}^{-n}$ (by previous case)

   Therefore $e' = \varphi(g^n)\,\{\varphi(g)\}^{-n}$

   Multiplying both sides by $\{\varphi(g)\}^n$, we get $\{\varphi(g)\}^n = \varphi(g^n)$.

   Hence the result.

3. Given that $g^n = e$.

   Consider $e' = \varphi(e) = \varphi(g^n) = (\varphi(g))^n$ (By Property (2))

   Therefore $o(\varphi(g))$ divides n.

4. To show that $\varphi^{-1}(g') = g \ker \varphi$

Let $x \in \varphi^{-1}(g')$ then, $\varphi(x) = g'$, i.e., $\varphi(x) = \varphi(g)$.

We now show that $x \in g \ker \varphi$.

As $\varphi(x) = \varphi(g)$. Therefore $e' = \{\varphi(g)\}^{-1} \varphi(x)$

$= \varphi(g^{-1}) \varphi(x)$ (Using Property (2))

$= \varphi(g^{-1}x)$ (As φ is homomorphism)

Thus $g^{-1}x \in \ker \varphi$ and so, $x \in g \ker \varphi$

Hence $\varphi^{-1}(g') \subseteq g \ker \varphi$ ...(1)

Now let $x \in g \ker \varphi$ then $x = gk$ for some $k \in \ker \varphi$ which gives $\varphi(k) = e'$.

To show that $x \in \varphi^{-1}(g')$.

We have $\varphi(x) = \varphi(gk) = \varphi(g) \varphi(k)$ ($\because$ φ is homomorphism)

$= \varphi(g)e' = \varphi(g) = g'$ (given)

Thus $x \in \varphi^{-1}(g')$ and so $g\ker \varphi \subseteq \varphi^{-1}(g')$ ...(2)

From (1) and (2), we get $\varphi^{-1}(g') = g \ker \varphi$.

Theorem 7.2: Let φ be a group homomorphism from G to G'. Then $\ker\varphi$ is a normal subgroup of G.

Proof: We have, $\ker\varphi = \{x \in G : \varphi(x) = e'\}$. Clearly $\ker\varphi \subseteq G$.

We first show that $\ker\varphi$ is a subgroup of G.

Since $\varphi(e) = e'$, so, $e \in \ker\varphi$. Thus, $\ker\varphi$ is non empty.

Let $x, y \in \ker\varphi$. Then, $\varphi(x) = e'$ and $\varphi(y) = e'$.

Now $\varphi(xy) = \varphi(x) \varphi(y) = e'e' = e'$ (As φ is homomorphism)

Therefore $xy \in \ker\varphi$

Further, $x \in \ker \varphi$ implies $\varphi(x) = e'$.

Then $\varphi(x^{-1}) = \{\varphi(x)\}^{-1} = \{e'\}^{-1} = e'$, and so, $x^{-1} \in \ker\varphi$.

Hence $\ker\varphi$ is a subgroup of G.

Now to show that $\ker\varphi$ is a normal subgroup of G we need to show that $g \ker\varphi\, g^{-1} \subseteq \ker\varphi$.

Let $a \in g \ker\varphi g^{-1}$ then $a = gkg^{-1}$ for some $k \in \ker\varphi$.

We will show that $a \in \ker\varphi$, i.e., $\varphi(a) = e'$

Consider $\varphi(a) = \varphi(gkg^{-1}) = \varphi(g) \varphi(k) \varphi(g^{-1})$

$= \varphi(g)\, e'\, \varphi(g^{-1})$ (since $k \in \ker \varphi$)

$= \varphi(g) \varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e'$

Thus $\varphi(a) = e'$ and hence $a \in \ker\varphi$.

Therefore $\ker\varphi$ is a normal subgroup of G.

Theorem 7.3: Let φ be a homomorphism from a group G to a group G'. Then φ^{-1} is homomorphism.

Proof: To show $\varphi^{-1}(xy) = \varphi^{-1}(x)\ \varphi^{-1}(y)\ \forall x, y \in G'$

Let $\varphi^{-1}(x) = a$ and $\varphi^{-1}(y) = b$, then, $\varphi(a) = x$ and $\varphi(b) = y$.

Therefore $xy = \varphi(a)\ \varphi(b) = \varphi(ab)$ ($\because$ φ is homomorphism)

Thus $ab = \varphi^{-1}(xy) = \varphi^{-1}(x)\ \varphi^{-1}(y)$

Hence φ^{-1} is homomorphism.

7.2 Properties of Subgroups under Homomorphism

We now study some simple, yet important results related to the properties of subgroups under homomorphism.

Theorem 7.4: Let φ be a homomorphism from a group G to a group G' and let H be a subgroup of G. Then

1. Homomorphic image of a subgroup is a subgroup, i.e., if H is a subgroup of G, then $\varphi(H) = \{\varphi(h) : h \in H\}$ is a subgroup of G'.
2. Homomorphic image of a cyclic subgroup is cyclic, i.e., if H is cyclic in G, then $\varphi(H)$ is cyclic in G'.
3. Homomorphic image of an abelian subgroup is abelian, i.e., if H is abelian, then so is $\varphi(H)$.
4. Homomorphic image of a normal subgroup in G is normal in the image of G, i.e., if H is a normal subgroup of G, then $\varphi(H)$ is a normal subgroup of $\varphi(G)$.
5. If $\ker\varphi$ has n elements, i.e., $o(\ker\varphi) = n$, then φ is an n to 1 mapping from G onto G'.
6. $\ker \varphi = \{e\}$ if and only if φ is one–one.
7. If $o(H) = n$, then $o(\varphi(H))$ divides n.
8. Homomorphic preimage of a subgroup is also a subgroup, i.e., if K is a subgroup of G' then $\varphi^{-1}(K) = \{k \in G : \varphi(k) \in K\}$ is a subgroup of G.
9. Homomorphic preimage of a normal subgroup is also a normal subgroup, i.e., if K is a normal subgroup of G', then $\varphi^{-1}(K) = \{k \in G : \varphi(k) \in K\}$ is a normal subgroup of G.

Proof:

1. To show that $\varphi(H) = \{\varphi(h) : h \in H\}$ is a subgroup of G'.

   As H is a subgroup of G, therefore, $e \in H$.

   Also $\varphi(e) = e'$, so $e' \in \varphi(H)$. Therefore, $\varphi(H)$ is non-empty.

Now let $x, y \in \varphi(H)$. To show that $xy \in \varphi(H)$.

As $x, y \in \varphi(H)$, so $x = \varphi(h_1)$ and $y = \varphi(h_2)$ for some $h_1, h_2 \in H$.

Then $xy = \varphi(h_1)\,\varphi(h_2) = \varphi(h_1h_2)$ ($\because$ φ is homomorphism)

Thus $xy \in \varphi(H)$ ($\because$ $h_1, h_2 \in H$ and $H \leq G$, so, $h_1h_2 \in H$)

Let $x \in \varphi(H)$. Then, $x = \varphi(h)$ for some $h \in H$

Thus $x^{-1} = \{\varphi(h)\}^{-1} = \varphi(h^{-1})$ and so $x^{-1} \in \varphi(H)$ (since $H \leq G$)

Therefore $\varphi(H)$ is a subgroup of G'.

2. Let $H = \langle a \rangle$ for some $a \in G$. We shall show that $\varphi(H) = \langle \varphi(a) \rangle$.

   Clearly, $\varphi(a) \in \varphi(H)$ and $\varphi(H)$ is a subgroup of G'. (by part 1)

   Therefore $\langle \varphi(a) \rangle \subseteq \varphi(H)$ ...(1)

   Now let $x \in \varphi(H)$. Then, $x = \varphi(h)$ for some $h \in H$.

   As $H = \langle a \rangle$ and $h \in H$, therefore $h = a^n$ for some $n \in \mathbb{Z}$.

   Then $x = \varphi(a^n) = \{\varphi(a)\}^n$ ($\because$ φ is homomorphism)

   Therefore $x \in \langle \varphi(a) \rangle$ and so, $\varphi(H) \subseteq \langle \varphi(a) \rangle$. ...(2)

   By (1) and (2), we have $\varphi(H) = \langle \varphi(a) \rangle$ and hence $\varphi(H)$ is cyclic.

   Remark: The converse of above statement may not be true.
   Consider the example:
   The group $(\mathbb{Z}, +)$ is cyclic, since $\mathbb{Z} = \langle 1 \rangle$.
   Let G be a group of 2×2 matrices over integers, under addition.
   The mapping $f : G \to \mathbb{Z}$ defined by $f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a$, is onto homomorphism.
   Hence $\mathbb{Z}$ is a homomorphic image of G, where $\mathbb{Z}$ is cyclic but G is not cyclic.

3. Given that $ab = ba$, for all $a, b \in H$. To show that $\varphi(H)$ is abelian.

   Let $x, y \in \varphi(H)$. We will show that $xy = yx$.

   As $x, y \in \varphi(H)$, we have $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in H$.

   Therefore, $xy = \varphi(a) \cdot \varphi(b) = \varphi(ab)$ ($\because$ φ is homomorphism)

   $= \varphi(ba)$ (given)

   $= \varphi(b)\varphi(a)$ ($\because$ φ is homomorphism)

   $= yx$

   Thus $\varphi(H)$ is abelian.

Remark: The converse of above statement may not be true.
It is illustrated by the following example:
Let $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$.
Then G is a non-abelian group under matrix multiplication.
Let G' be the group of non-zero real numbers under multiplication.
Clearly G' is abelian.
The mapping $f : G \to G'$ defined by $f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$
is an onto homomorphism.
Hence G' is a homomorphic image of G, where G' is abelian but G is non-abelian.

4. Let H be a normal subgroup of G.

   To show that $\varphi(H)$ is a normal subgroup of $\varphi(G)$, we need to show that $g' \varphi(H)(g')^{-1} \subseteq \varphi(H)$, $\forall\ g' \in \varphi(G)$.

   Let $g' = \varphi(g)$ for some $g \in G$.

   Now let $x \in g' \varphi(H)(g')^{-1}$ then, $x = g' \varphi(h)(g')^{-1}$ for some $h \in H$.

   Thus $x = \varphi(g)\ \varphi(h)\ (\varphi(g))^{-1} = \varphi(g)\ \varphi(h)\ \varphi(g^{-1})$
   $= \varphi(ghg^{-1})$ ($\because$ φ is homomorphism)

   As $h \in H$, $g \in G$ and H is a normal subgroup of G, so $ghg^{-1} \in H$.

   Therefore $x = \varphi(ghg^{-1}) \in \varphi(H)$ and so, $g' \varphi(H)\ (g')^{-1} \subseteq \varphi(H)$.

   Thus $\varphi(H)$ is a normal subgroup of $\varphi(G)$.

5. Let $g' \in G'$. To show that there are n elements mapped to g'.

   Now $\varphi^{-1}(g') = g \ker \varphi$

   So $o(\varphi^{-1}(g')) = o(g \ker \varphi) = o(\ker \varphi) = n$,

   i.e., n elements are mapped to g' and so, φ is an n to 1 map.

6. Let $\ker \varphi = \{e\}$ and let $\varphi(x) = \varphi(y)$ for some $x, y \in G$.

   Then $\varphi(x)(\varphi(y))^{-1} = e'$

   $\Rightarrow$ $\varphi(x)\ \varphi(y^{-1}) = e'$

   $\Rightarrow$ $\varphi(xy^{-1}) = e'$ ($\because$ φ is homomorphism)

   $\Rightarrow$ $xy^{-1} \in \ker \varphi = e$

   So $xy^{-1} = e$ and hence $x = y$.

   Therefore φ is one–one.

Conversely, let φ be one–one. Let $x \in \ker \varphi$ be any element.

$\Rightarrow \quad \varphi(x) = e'$

$\Rightarrow \quad \varphi(x) = \varphi(e)$

$\Rightarrow \quad x = e$ (As φ is one–one)

Therefore $\ker\varphi = \{e\}$.

7. Since $o(H) = n$, we have $h^n = e$, $\forall\ h \in H$

   Thus, $e' = \varphi(e) = \varphi(h^n) = \{\varphi(h)\}^n$, $\forall\ h \in H$

   Therefore, $o(\varphi(H))$ divides n.

8. To show that $\varphi^{-1}(K) = \{k \in G : \varphi(k) \in K\}$ is a subgroup of G.

   Now, $\varphi^{-1}(K)$ is non-empty, because $e \in \varphi^{-1}(K)$ as $\varphi(e) = e' \in K$.

   Let $x, y \in \varphi^{-1}(K)$, then $x = \varphi^{-1}(k_1)$ and $y = \varphi^{-1}(k_2)$ for some $k_1, k_2 \in K$.

   Thus $\varphi(x) = k_1$ and $\varphi(y) = k_2$.

   Consider $\varphi(xy) = \varphi(x)\ \varphi(y)$ ($\because$ φ is homomorphism)

   $= k_1\ k_2$

   Therefore $\varphi(xy) \in K$ and hence $xy \in \varphi^{-1}(K)$.

   Now let $x \in \varphi^{-1}(K)$, then $x = \varphi^{-1}(k)$ for some $k \in K$.

   Thus $\varphi(x) = k$.

   So $\varphi(x^{-1}) = \{\varphi(x)\}^{-1} = k^{-1} \in K$ ($\because\ K \leq G'$)

   Therefore $x^{-1} \in \varphi^{-1}(K)$.

   Thus $\varphi^{-1}(K) = \{k \in G : \varphi(k) \in K\}$ is a subgroup of G.

9. To show $\varphi^{-1}(K) = \{k \in G : \varphi(k) \in K\}$ is a normal subgroup of G, we need to show that $g\varphi^{-1}(K)g^{-1} \subseteq \varphi^{-1}(K)$, where $g = \varphi^{-1}(g')$ for some $g' \in G'$ or $\varphi(g) = g'$, i.e., we need to show that $g\varphi^{-1}(k)g^{-1} \in \varphi^{-1}(K)$, $\forall\ k \in K$.

   Now $g\varphi^{-1}(k)g^{-1} = \varphi^{-1}(g')\ \varphi^{-1}(k)\ (\varphi^{-1}(g'))^{-1}$

   $= \varphi^{-1}(g'k)\ [\varphi^{-1}(g')^{-1}]$ ($\because\ \varphi^{-1}$ is homomorphism)

   $= \varphi^{-1}(g'k(g')^{-1}) \in \varphi^{-1}(K)$ as $g'k(g')^{-1} \in K$ as $K \trianglelefteq G'$.

   Thus, $g\varphi^{-1}(K)g^{-1} \subseteq \varphi^{-1}(K)$

   Thus, $\varphi^{-1}(K) = \{k \in G : \varphi(k) \in K\}$ is a normal subgroup of G.

ILLUSTRATIONS:

1. Define a map $f : \mathbb{C}^* \to \mathbb{C}^*$ by $f(x) = x^4$

   Then $f(xy) = (xy)^4 = x^4y^4 = f(x)f(y)$ ($\because$ $\mathbb{C}^*$ is abelian)

   Thus, f is a homomorphism.

   Also, $\ker f = \{x \in \mathbb{C}^* : f(x) = 1\} = \{x \in \mathbb{C}^* : x^4 = 1\} = \{1, -1, -i, i\}$

   Thus, f is a 4-to-1 mapping.

   Let $g' = 2$, we find all those elements that map to 2, i.e., we need to find $f^{-1}(2)$.

   We have $f^{-1}(2) = g \ker f$, where $f(g) = g'$

   Since $f(\sqrt[4]{2}) = (\sqrt[4]{2})^4 = 2$, let us take $g = \sqrt[4]{2}$

   $\therefore f^{-1}(2) = g\ker f = \sqrt[4]{2}\{1, -1, i, -i\} = \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$

   Now, let $H = \langle a \rangle$, where $a = \cos 30° + i \sin 30°$

   We have $a^{12} = (\cos 30° + i \sin 30°)^{12} = \cos 360° + i \sin 360° = 1$

   $\Rightarrow$ $o(a) = 12$. Thus $o(H) = 12$

   Also, $f(H) = \{f(h) : h \in H\} = \langle f(a) \rangle = \langle a^4 \rangle \equiv \langle b \rangle$, where $b = a^4 = \cos 120° + i \sin 120°$.

   Now $b^3 = 1$, so $o(f(H)) = 3$

   This gives that $o(f(H))$ divides $o(H)$.

2. Let $g : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ be defined by $g(x) = 3x \bmod 12$.

   Then $g(x \oplus_{12} y) = 3(x + y) \bmod 12$

   $= (3x \bmod 12 + 3y \bmod 12) \bmod 12$

   $= g(x) \oplus_{12} g(y)$

   Thus, g is a homomorphism.

   Also, $\ker g = \{x \in \mathbb{Z}_{12} : g(x) = 0\} = \{x \in \mathbb{Z}_{12} : 3x \bmod 12 = 0\}$

   $= \{0, 4, 8\}$

   Thus, g is a 3-to-1 mapping.

   Further, let $g' = 6$. Now $g(2) = 3.2 \bmod 12 = 6$

   $\Rightarrow g^{-1}(6) = 2 + \ker g = \{2, 6, 10\}$

   Let $H = \langle a \rangle$, where $a = 2$, then $H = \{2, 4, 6, 8, 10, 0\}$

   Also $\langle g(H) \rangle = \langle g(a) \rangle = \langle g(2) \rangle = \langle 6 \rangle = \{6, 0\}$

   This implies that $o(g(H))$ divides $o(H)$.

   Also $o(g(2)) | o(2)$

   Now, let $K = \{0, 6\}$ then $g^{-1}(K) = \{0, 2, 4, 6, 8, 10\}$ is a subgroup of $\mathbb{Z}_{12}$.

7.3 Isomorphism of Groups

The notion of isomorphism—of having the same structure—is central to every branch of mathematics. It is an expression of the simple fact that objects may be different in substance but identical in form.

In abstract algebra, we say that two mathematical objects are isomorphic if they have the same structure. An isomorphism is a mapping between two such objects which preserves the structure of the objects.

Isomorphisms therefore naturally appear in group theory, and can be defined as follows:

Definition 7.3: A mapping $f : G_1 \to G_2$ is said to be an **isomorphism** if f is one-one, onto and homomorphism.

So by an isomorphism between two groups we mean a one-to-one correspondence between them which transforms one of the groups into the other.

Definition 7.4: Two groups G_1 and G_2 are said to be **isomorphic**, if there is an isomorphism of G_1 onto G_2.

We symbolize this fact by writing $\boldsymbol{G_1 \cong G_2}$ to be read, "**G_1 is isomorphic to G_2**".

Examples of Isomorphism:

1. Let G be the group of integers under addition and G' be the group of even integers under addition.

   Define $\varphi : G \to G'$ by $\varphi(x) = 2x$.

   Then, $\varphi(x) = \varphi(y) \Rightarrow 2x = 2y \Rightarrow x = y$. So φ is one–one.

   Now let $y \in G'$, then $y = 2m$ for some $m \in \mathbb{Z}$. So there exists $m \in G$ such that $\varphi(m) = 2m = y$. Thus φ is onto.

   Also $\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y)$

   Therefore φ is a homomorphism and hence an isomorphism.

2. Let G be the group of real numbers under addition and G' be the group of positive real numbers under multiplication.

   Define $\varphi : G \to G'$ by $\varphi(x) = 2^x$. Then, φ is well defined as

   $$x = y \Rightarrow 2^x = 2^y \Rightarrow \varphi(x) = \varphi(y).$$

   Also φ is one – one as

   $\varphi(x) = \varphi(y) \Rightarrow 2^x = 2^y \Rightarrow \log 2^x = \log 2^y \Rightarrow x \log 2 = y \log 2 \Rightarrow x = y.$

   φ is onto as let $y \in G'$. To find $x \in G$ such that $y = 2^x$

   i.e., $\log y = x \log 2$, i.e., $x = \dfrac{\log y}{\log 2} = \log_2 y$.

   Thus for $y \in G'$, there exists $x = \log_2 y \in G$ such that $\varphi(x) = y$.

Also φ is homomorphism as for $x, y \in G$

$$\varphi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x) \cdot \varphi(y)$$

Therefore φ is an isomorphism.

3. Let G be the group of real numbers under addition.

   Define $\varphi : G \to G$ by $\varphi(x) = x^3$. Then φ is not an isomorphism as φ is one-one and onto, but

   $$\varphi(x + y) = (x + y)^3 \neq x^3 + y^3 = \varphi(x) + \varphi(y), \ \forall\ x, y \in G.$$

4. $U(10) \ncong U(12)$.

   Note that $x^2 = 1, \ \forall\ x \in U(12)$ ...(1)

   Let, if possible, $U(10) \cong U(12)$ then there exists a mapping

   $\varphi : U(10) \to U(12)$ such that φ is one–one, onto and homomorphism.

   Consider $\varphi(9) = \varphi(3.3) = \varphi(3)\ \varphi(3) = (\varphi(3))^2 = 1$

   (by (1))

   Also $\varphi(1) = \varphi(1.1) = \varphi(1)\ \varphi(1) = (\varphi(1))^2 = 1$

   Here $\varphi(9) = \varphi(1)$ but $9 \neq 1$. Thus, φ is not one – one, a contradiction.

   Hence $U(10) \ncong U(12)$.

5. Let $G = (\mathbb{Q}, +)$ and $G' = (\mathbb{Q}^*, .)$

   Then $G \ncong G'$. Let, if possible, $G \cong G'$.

   Then there exists a mapping $\varphi : G \to G'$ such that φ is one –one, onto and homomorphism.

   Now as $-1 \in \mathbb{Q}^*$ and φ is onto, therefore, there exists some $a \in \mathbb{Q}$ such that $\varphi(a) = -1$.

   Then $\varphi\left(\frac{a}{2} + \frac{a}{2}\right) = -1$. So, $\varphi\left(\frac{a}{2}\right).\varphi\left(\frac{a}{2}\right) = -1$

   Thus $\left(\varphi\left(\frac{a}{2}\right)\right)^2 = -1$ (absurd), as no rational number squares to -1.

   Therefore $\mathbb{Q} \ncong \mathbb{Q}^*$.

Problem 7.2 Show that $(\mathbb{R}, +)$ is not isomorphic to $(\mathbb{R}^*, \cdot)$.

Solution Suppose there is an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}^*, \cdot)$.

Since $(-1) \in \mathbb{R}^*$ and $(-1)^2 = 1$, so $o(-1) = 2$.

But $(\mathbb{R}, +)$ has no element of order 2 because if $o(x) = 2$ then $2x = 0$

This gives $x + x = 0$ and so $x = 0$, which is not of order 2, a contradiction.

Hence $(\mathbb{R}, +) \ncong (\mathbb{R}^*, \cdot)$.

7.4 Some Theorems Based on Isomorphism of Groups

We will discuss some important theorems based on isomorphism of groups and properties of isomorphism.

Theorem 7.5: (First Isomorphism Theorem)†

Let $f : G \to G'$ be a group homomorphism with $K = \ker f$. Then $\frac{G}{K} \cong f(G)$

Proof: Since $\ker f \trianglelefteq G$, so, $K \trianglelefteq G$ and thus G/K is defined.

Define a map $\varphi : G/K \to f(G)$ such that $\varphi(Ka) = f(a)$, $\forall\ a \in G$.

We now show that φ is an isomorphism. For this we need to show that φ is one-one, onto and homomorphism.

We have $Ka = Kb$, $a, b \in G$

$\Leftrightarrow \quad ab^{-1} \in K = \ker f$

$\Leftrightarrow \quad f(ab^{-1}) = e'$

$\Leftrightarrow \quad f(a)f(b^{-1}) = e'$ $\quad (\because f$ is homomorphism)

$\Leftrightarrow \quad f(a)\,(f(b))^{-1} = e'$

$\Leftrightarrow \quad f(a) = f(b)$

$\Leftrightarrow \quad \varphi(Ka) = \varphi(Kb)$

So, φ is well defined and one-one.

Also, $\varphi(G/K) = \{\varphi(Ka) : a \in G\} = \{f(a) : a \in G\} = f(G)$

Thus, φ is onto.

Also, $\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb)$

Therefore φ is homomorphism and hence, φ is isomorphism.

Theorem 7.6: Let $f : G \to G'$ be an onto homomorphism from a group G to a group G' with $K = \ker f$. Then $\frac{G}{K} \cong G'$.

Since the mapping f is onto, therefore $f(G) = G'$.

Thus, from the above theorem, $\frac{G}{K} \cong f(G) = G'$

It asserts that every homomorphic image of G is isomorphic to a quotient group of G.

---

† The First Isomorphism Theorem is popularly known as Fundamental Theorem of Homomorphism.

THEOREM 7.7: (Second Isomorphism Theorem)[†]

Let H and K be two subgroups of a group G, where H is normal in G, then

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

Proof: Clearly $H \cap K \trianglelefteq K$ and $H \subseteq HK \subseteq G$, therefore H will be normal in HK.

Define a map $f : K \to \frac{HK}{H}$ such that $f(k) = Hk$, $k \in K$.

Then f is well defined as $k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow f(k_1) = f(k_2)$, $\forall\ k_1, k_2 \in K$.

Also $f(k_1k_2) = Hk_1k_2 = Hk_1 \cdot Hk_2 = f(k_1)\, f(k_2)$, $\forall\ k_1, k_2 \in K$.

Therefore f is a homomorphism.

Further f is onto as let $Hx \in \frac{HK}{H}$ be any element. Then, $x \in HK \Rightarrow x = hk$ for some $h \in H$, $k \in K$.

Now $Hx = Hhk = Hk = f(k)$ ($\because\ h \in H$, so, $Hh = H$)

So for $Hx \in \frac{HK}{H}$, there exists $k \in K$ such that $f(k) = Hx$.

So by Theorem 7.6 $\frac{HK}{H} \cong \frac{K}{\ker f}$. ...(1)

Now $k \in \ker f \Leftrightarrow f(k) = H$

$\Leftrightarrow Hk = H$

$\Leftrightarrow k \in H$

$\Leftrightarrow k \in H \cap K$ ($\because\ k \in K$ as $\ker f \subseteq K$)

Therefore $\ker f = H \cap K$

Hence by (1), $\frac{HK}{H} \cong \frac{K}{H \cap K}$.

THEOREM 7.8: (Third Isomorphism Theorem)[††]

If H and K are two normal subgroups of a group G such that $H \subseteq K$, then $\frac{G}{K} \cong \frac{G/H}{K/H}$.

Proof: Define a map $f : \frac{G}{H} \to \frac{G}{K}$ such that $f(Ha) = Ka$, $a \in G$.

Then for all $a, b \in G$, $Ha = Hb \Rightarrow ab^{-1} \in H \subseteq K \Rightarrow Ka = Kb$

[†] The Second Isomorphism Theorem is popularly known as Diamond Isomorphism Theorem.

[††] The Third Isomorphism Theorem is popularly known as Freshman Theorem.

Thus $f(Ha) = f(Hb)$. Therefore, f is well defined.

Also f is homomorphism as

$f(HaHb) = f(Hab) = Kab = KaKb = f(Ha)f(Hb), a,b \in G$.

f is clearly onto, as for any $Ka \in G/K$, Ha is the required preimage.

Therefore by Theorem 7.6 $\dfrac{G}{K} \cong \dfrac{G/H}{\ker f}$ ...(1)

We claim that $\ker f = \dfrac{K}{H}$.

Now $Ha \in \ker f \Leftrightarrow f(Ha) = K$ (identity of G/K)

$\Leftrightarrow \quad Ka = K \Leftrightarrow a \in K \Leftrightarrow Ha \in K/H$.

Therefore $\ker f = \dfrac{K}{H}$.

So by (1), $\dfrac{G}{K} \cong \dfrac{G/H}{K/H}$.

Since $K/H = \ker f$, and $\ker f \trianglelefteq \dfrac{G}{H}$, so, $\dfrac{K}{H} \trianglelefteq \dfrac{G}{H}$, thus $\dfrac{G/H}{K/H}$ is defined.

PROBLEM 7.3 Show that every normal subgroup of a group G is the kernel of homomorphism of G.

SOLUTION Let H be a normal subgroup of G.

Define a map $f : G \to G/H$ by $f(g) = gH$

Then $f(gh) = (gh)H = (gH)(hH) = f(g)f(h)$

Thus f is a homomorphism.

For any $gH \in G/H$, there exists $g \in G$ such that $f(g) = gH$. Thus f is onto.

Then, $\ker f = \{g \in G : f(g) = H\} = \{g \in G : gH = H\} = \{g \in G : g \in H\} = H$.

The mapping f is called a natural homomorphism from G to G/H.

PROBLEM 7.4 Using Theorem 7.6, show that

$$o(A_n) = \frac{o(S_n)}{2}.$$

SOLUTION Let $G = \{1, -1\}$ be a group under multiplication.

Define a map $f : S_n \to G$ such that

$$f(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

We claim that f is homomorphism.

Let $\sigma, \eta \in S_n$.

Case I: Both σ and η are even. Then $\sigma\eta$ is even.

Thus, $f(\sigma\eta) = 1 = 1.1 = f(\sigma)\, f(\eta)$

Case II: Both σ and η are odd. Then $\sigma\eta$ is even.

Thus $f(\sigma\eta) = 1 = (-1)\cdot(-1) = f(\sigma)\, f(\eta)$

Case III: σ is even and η is odd. Then $\sigma\eta$ is odd.

Thus $f(\sigma\eta) = -1 = 1(-1) = f(\sigma)\, f(\eta)$

Thus f is homomorphism.

Clearly f is onto. Therefore by Theorem 7.6, $G \cong \dfrac{S_n}{\ker f}$.

Now $\sigma \in \ker f \Leftrightarrow f(\sigma) = 1 \Leftrightarrow \sigma$ is even $\Leftrightarrow \sigma \in A_n$.

Thus $\ker f = A_n$.

Therefore $\dfrac{S_n}{A_n} \cong G$.

$$\Rightarrow o\left(\frac{S_n}{A_n}\right) = o(G) = 2$$

$$\Rightarrow \quad \frac{o(S_n)}{o(A_n)} = 2$$

$$\Rightarrow \quad o(A_n) = \frac{o(S_n)}{2}.$$

PROBLEM 7.5 Show that any infinite cyclic group G is isomorphic to $(\mathbb{Z}, +)$

SOLUTION Let $G = \langle a \rangle$ be the given infinite cyclic group.

Define a mapping $f : G \to \mathbb{Z}$ such that $f(a^i) = i$.

Then $a^i = a^j \Rightarrow i = j$ as if $i \neq j$ then $a^{i-j} = e$ implying $o(a)$ is finite

So $o(G)$ is finite, a contradiction. Therefore $i = j$.

Thus $f(a^i) = f(a^j)$ and hence f is well defined.

Clearly f is onto as every element in $\mathbb{Z}$ has a preimage in G.

Also f is one-one as $f(a^i) = f(a^j) \Rightarrow i = j \Rightarrow a^i = a^j$

Further, f is homomorphism as $f(a^i\, a^j) = f(a^{i+j}) = i + j = f(a^i) + (a^j)$.

Therefore $G \cong \mathbb{Z}$.

PROBLEM 7.6 Show that a finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

SOLUTION Let $G = \langle a \rangle$ be a finite cyclic group of order n such that $o(G) = o(a) = n$.

Then $G = \{e, a, a^2, \ldots, a^{n-1}\}$ and $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Define a map $f : G \to \mathbb{Z}_n$, such that $f(a^i) = i$.

Then f is well defined as

$$a^i = a^j \Rightarrow \log a^i = \log a^j \Rightarrow i \log a = j \log a \Rightarrow i = j$$

Also f is one–one as $f(a^i) = f(a^j) \Rightarrow i = j \Rightarrow a^i = a^j$.

Further f is onto as for $i \in \mathbb{Z}_n$, there exists $a^i \in G$ such that $f(a^i) = i$.

Now $f(a^i \cdot a^j) = f(a^{i+j}) = i \oplus j = f(a^i) \oplus f(a^j)$. So f is a homomorphism.

(For example $f(a^6\, a^7) = f(a^{13}) = 13 \equiv 3 (\text{mod } 10)$ and $f(a^6) \oplus f(a^7) = 6 \oplus 7 = 13 \equiv 3 \text{ (mod (10))}$

Thus $G \cong Z_n$. .

PROBLEM 7.7 Prove that any finite cyclic group of order n is isomorphic to $\dfrac{\mathbb{Z}}{\langle n \rangle}$.

SOLUTION Let $G = \langle a \rangle$ be a cyclic group of order n.

Define $f : \mathbb{Z} \to G$ such that $f(m) = a^m$.

Then f is well defined as $m = n \Rightarrow a^m = a^n \Rightarrow f(m) = f(n)$.

Now $f(m+k) = a^{m+k} = a^m \cdot a^k = f(m) \cdot f(k)$

Therefore f is homomorphism.

Clearly f is onto as every element in G has a preimage in $\mathbb{Z}$.

Therefore by Theorem 7.6, $G \cong \dfrac{\mathbb{Z}}{\ker f}$

Now, $m \in \ker f \Leftrightarrow f(m) = e \Leftrightarrow a^m = e \Leftrightarrow o(a) \mid m \quad \Leftrightarrow n/m \Leftrightarrow \quad m \in \langle n \rangle$

Thus $\ker f = \langle n \rangle$. Hence $G \cong \dfrac{\mathbb{Z}}{\langle n \rangle}$.

In the following theorem, it is shown that isomorphism is an equivalence relation among groups.

THEOREM 7.9: The relation '$\cong$' of being "isomorphic to" is an equivalence relation (on the collection of all groups).

Proof: Let $\mathcal{G}$ denote the collection of all groups.

To show that '$\cong$' is an equivalence relation on $\mathcal{G}$.

Reflexive: To show $G \cong G$, $\forall G \in \mathcal{G}$.

Define a mapping $g : G \to G$ as $g(x) = x$, $\forall\ x \in G$

Then, clearly $G \cong G$.

Symmetry: Let $G, G' \in \mathcal{G}$ such that $G \cong G'$, i.e., there exists an isomorphism $\varphi : G \to G'$.

As φ is one–one and onto, so it is invertible, i.e., there exists a mapping $\varphi^{-1} : G' \to G$ which is also one–one and onto. Further if $\varphi : G \to G'$ is a homomorphism then $\varphi^{-1} : G' \to G$ also a homomorphism.

Thus φ^{-1} is an isomorphism of G' onto G. Thus, $G' \cong G$.

Transitivity: Let G, G' and $G'' \in \mathcal{G}$ such that $G \cong G'$ and $G' \cong G''$,

i.e., there exists an isomorphism, say $\varphi : G \to G'$ and an isomorphism, say $\psi : G' \to G''$.

Consider the composition $\psi \circ \varphi : G \to G''$ defined as

$$(\psi \circ \varphi)(x) = \psi(\varphi(x))$$

Then $\psi \circ \varphi$ is well defined and one–one as for all $x, y \in G$, we have

$$(\psi \circ \varphi)(x) = (\psi \circ \varphi)(y)$$

$\Leftrightarrow$ $\psi(\varphi(x)) = \psi(\varphi(y))$

$\Leftrightarrow$ $\varphi(x) = \varphi(y)$ (since ψ is one–one)

$\Leftrightarrow$ $x = y$ (since φ is one–one)

$\psi \circ \varphi$ is onto as let $g'' \in G''$, since $\psi : G' \to G''$ is onto, so there exists $g' \in G'$ such that $\psi(g') = g''$.

Also as $\varphi : G \to G'$ is onto, there exists $g \in G$ such that $\varphi(g) = g'$

Thus $g'' = \psi(\varphi(g)) = (\psi \circ \varphi)(g)$.

So for $g'' \in G''$, there exists $g \in G$ such that $(\psi \circ \varphi)(g) = g''$.

We now show that $\psi \circ \varphi$ is a homomorphism. For all $x, y \in G$,

$$\begin{aligned}(\psi \circ \varphi)(xy) &= \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) && (\because\ \varphi \text{ is homomorphism})\\ &= \psi(\varphi(x)) \cdot \psi(\varphi(y)) && (\because\ \psi \text{ is homomorphism})\\ &= (\psi \circ \varphi)(x) \cdot (\psi \circ \varphi)(y)\end{aligned}$$

Therefore $\psi \circ \varphi$ is an isomorphism of G onto G''. Hence $G \cong G''$.

Remark: Since $G \cong \dfrac{\mathbb{Z}}{\langle n \rangle}$ and also $G \cong \mathbb{Z}_n$. Therefore by transitivity $\mathbb{Z}_n \cong \dfrac{\mathbb{Z}}{\langle n \rangle}$.

In the following theorem, given by Arthur Cayley, about 100 years ago, it is shown that every group is isomorphic (or is a carbon copy of) to a group of permutations. This great result is a classic theorem of modern algebra.

Theorem 7.10: (Cayley's Theorem)

Every group G is isomorphic to a permutation group.

Proof: Let G be the given group and $A(G)$ be the group of all permutations of the set G.

For any $a \in G$, define $T_a : G \to G$ such that $T_a(x) = ax$, $\forall\ x \in G$

Then $x = y \Rightarrow ax = ay \Rightarrow T_a(x) = T_a(y)\ \forall\ x, y \in G$, therefore T_a is well defined.

Again $T_a(x) = T_a(y) \Rightarrow ax = ay \Rightarrow x = y$ (cancellation law in group G).

So T_a is one–one.

Also for any $y \in G$, $a^{-1}y \in G$ and $T_a(a^{-1}y) = a(a^{-1}y) = y$

We find that $a^{-1}y$ is preimage of y, thus T_a is onto and hence T_a is a permutation on G.

Let K be the set of all such permutations, then $K \subseteq A(G)$.

Claim: K is a subgroup of $A(G)$.

We have $K \neq \phi$ as $T_e \in K$. Let T_a, $T_b \in K$ be any arbitrary elements.

Then for all x, $T_b \circ T_{b^{-1}}(x) = T_b(T_{b^{-1}}(x)) = T_b(b^{-1}x) = b(b^{-1}x) = ex = T_e(x)$

So $T_b \circ T_{b^{-1}} = T_e$. Hence $T_{b^{-1}} = (T_b)^{-1}$.

Again, $T_a \circ T_b(x) = T_a\,(T_b(x)) = T_a(bx) = abx = T_{ab}(x)\ \forall x$.

Thus $T_a \circ T_b = T_{ab}$.

Hence $T_a \circ (T_b)^{-1} = T_a \circ T_{b^{-1}} = T_{ab^{-1}} \in K$.

Therefore, K is a subgroup of $A(G)$.

Define a mapping $\varphi : G \to K$ such that $\varphi(a) = T_a$.

Then for all $a, b \in G$, $\varphi(a) = \varphi(b)$

$\Leftrightarrow \quad T_a = T_b$

$\Leftrightarrow \quad T_a(x) = T_b(x)$

$\Leftrightarrow \quad ax = bx\ \forall\ x$

$\Leftrightarrow \quad a = b$

Thus φ is well defined and one–one.

Also φ is onto, as for any $T_a \in K$, $a \in G$ is the required preimage.

Now $\varphi(ab) = T_{ab} = T_a \circ T_b = \varphi(a)\ \varphi(b)$. Thus φ is homomorphism, and hence φ is an isomorphism.

Now K being a subgroup of a permutation group is a permutation group.

Thus $G \cong K$ (permutation group).

Problem 7.8 Determine all homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$.

Solution Let $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$ be any homomorphism. Let $\varphi(1) = a$.

For any $x \in \mathbb{Z}_{12}$, $\varphi(x) = \varphi(\underbrace{1+1+...+1}_{x \text{ times}}) = \underbrace{\varphi(1)+\varphi(1)+....+\varphi(1)}_{x \text{ times}} = x\,\varphi(1) = xa$.

Therefore $\varphi(x) = xa$.

Now, $o(1) = 12$, and $o(\varphi(1))|12$

i.e., $o(a)|12$ (Using property 7 of theorem 7.3)

Also since $a \in \mathbb{Z}_{30}$ so, $o(a)|30$. (by Lagrange's Theorem)

Now $o(a)|12$ and $o(a)|30$. Thus $o(a) = 1, 2, 3, 6$.

If $o(a) = 1$, then $1a = 0$ and so $a = 0$.

If $o(a) = 2$, then $2a = 0$, so $a = 15$ (since $2 \times 15 = 30 \bmod 30 = 0$)

If $o(a) = 3$, then $3a = 0$, so $a = 10, 20$.

If $o(a) = 6$, then $6a = 0$, so $a = 5, 25$.

Thus, a will have values 0, 15, 10, 15, 20, 25.

Therefore there exists 6 homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$.

Problem 7.9 Determine all homomorphisms from $\mathbb{Z}_8$ to $\mathbb{Z}_{20}$. How many of them are onto?

Solution Let $\varphi : \mathbb{Z}_8 \to \mathbb{Z}_{20}$ be any homomorphism. Let $\varphi(1) = a$.

For any x, $\varphi(x) = \varphi(\underbrace{1+1+...+1}_{x \text{ times}}) = \underbrace{\varphi(1)+\varphi(1)+....+\varphi(1)}_{x \text{ times}} = x\varphi(1) = xa$.

Therefore $\varphi(x) = xa$.

Now $o(1) = 8$, so $o(\varphi(1))|8$,

i.e., $o(a)|8$ (Using property 7 of theorem 7.3)

Also since $a \in \mathbb{Z}_{20}$, $o(a)|20$ (by Lagrange's Theorem)

Now $o(1)|8$, and $o(a)|20$. Thus $o(a) = 1, 2, 4$.

If $o(a) = 1$, then $1 \cdot a = 0$, so $a = 0$.

If $o(a) = 2$, then $2a = 0$ and so $a = 10$.

If $o(a) = 4$, then $4a = 0$, i.e., $a = 5, 10, 15$.

So a will have values 0, 5, 10, 15.

Thus there exist 4 homomorphisms from $\mathbb{Z}_8$ to $\mathbb{Z}_{20}$.

Let, if possible, $\varphi : \mathbb{Z}_8 \to \mathbb{Z}_{20}$ be onto.

Then by Theorem 7.6, we have, $\frac{\mathbb{Z}_8}{\ker \varphi} \cong \mathbb{Z}_{20}$

$\Rightarrow \quad o\left(\frac{\mathbb{Z}_8}{\ker \varphi}\right) = o(\mathbb{Z}_{20})$.

Thus $\quad o(\mathbb{Z}_{20}) = \frac{o(\mathbb{Z}_8)}{o(\ker \varphi)}$

This gives $o(\ker \varphi) = \frac{8}{20} = \frac{2}{5}$, which is not possible.

Therefore φ is not onto.

Remark: From above two problems, we observe that the number of homomorphism from $\mathbb{Z}_m$ to $\mathbb{Z}_n$ is same as gcd(m, n).

In the following theorem, some general properties of isomorphism are stated and proved.

Theorem 7.11: Let $\varphi : G \to G'$ be an isomorphism. Then

1. G is abelian if and only if G' is abelian.
2. Isomorphism preserves order, i.e., $o(\varphi(a)) = o(a)$, $\forall a \in G$.
3. φ^{-1} is an isomorphism from G' to G.
4. G is cyclic if and only if G' is cyclic.

Proof:

1. Let G be abelian.

   To show that G' is abelian, i.e., $xy = yx$, $\forall\ x, y \in G'$.

   Since $x, y \in G'$, $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in G$.

   Since G is abelian, therefore $ab = ba$.

   Thus, $\varphi(ab) = \varphi(ba)$ ($\because$ φ is well defined)

   $\Rightarrow \varphi(a)\ \varphi(b) = \varphi(b)\ \varphi(a)$ ($\because$ φ is homomorphism)

   $\Rightarrow xy = yx$.

   Therefore G' is abelian.

   Conversely, let G' be abelian.

   To show that G is abelian, i.e., $ab = ba$, $\forall\ a, b \in G$.

   Since $a, b \in G$, so, $\varphi(a), \varphi(b) \in G'$

   Since G' is abelian, we have $\varphi(a)\ \varphi(b) = \varphi(b)\ \varphi(a)$

   $\Rightarrow \varphi(ab) = \varphi(ba)$ ($\because$ φ is homomorphism)

   $\Rightarrow ab = ba$ ($\because$ φ is one–one)

   Thus G is abelian.

2. Let $o(a) = n$. To show that $o(\varphi(a)) = n$

   Since $o(a) = n$ we have $a^n = e$.

   This gives, $\varphi(a^n) = \varphi(e)$ ($\because$ φ is well defined)

   Then $\{\varphi(a)\}^n = e'$ and so, $o(\varphi(a)) | n$.

   Let $o(\varphi(a)) = k$, then $k | n$ ...(1)

   Also $\{\varphi(a)\}^k = e'$, so $\varphi(a^k) = \varphi(e)$

   Since φ is one–one, we have $a^k = e$

   But $o(a) = n$, so $n | k$. ...(2)

   From (1) and (2), we get $n = k$, i.e., $o(\varphi(a)) = n$.

3. To show $\varphi^{-1} : G' \to G$ is an isomorphism.

   Well defined: Let $a, b \in G'$. Then, $a = \varphi(g_1)$ and $b = \varphi(g_2)$ for some $g_1, g_2 \in G$.

   Now $a = b \Rightarrow \varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$ ($\because$ φ is one-one)

   $\Rightarrow \varphi^{-1}(a) = \varphi^{-1}(b)$

   One-one: Let $a, b \in G'$ be any elements.

   Then $a = \varphi(g_1)$ and $b = \varphi(g_2)$ for some $g_1, g_2 \in G$. So, $\varphi^{-1}(a) = g_1$ and $\varphi^{-1}(b) = g_2$.

   Now $\varphi^{-1}(a) = \varphi^{-1}(b) \Rightarrow g_1 = g_2 \Rightarrow \varphi(g_1) = \varphi(g_2)$ ($\because$ φ is well defined)

   $\Rightarrow a = b$.

   Onto: Since φ is onto, so $\varphi(g) = g'$ gives $\varphi^{-1}(g') = g$

   Thus for all $g \in G$, there exists $g' \in G'$ such that $\varphi^{-1}(g') = g$.

   Homomorphism: Let $a, b \in G'$ then $a = \varphi(g_1)$ and $b = \varphi(g_2)$ for some $g_1, g_2 \in G$.

   This gives, $\varphi^{-1}(a) = g_1$ and $\varphi^{-1}(b) = g_2$.

   Now $ab = \varphi(g_1) \cdot \varphi(g_2) = \varphi(g_1 g_2)$ ($\because$ φ is homomorphism)

   Thus $\varphi^{-1}(ab) = g_1 g_2 = \varphi^{-1}(a)\ \varphi^{-1}(b)$.

   Thus $\varphi^{-1} : G' \to G$ is an isomorphism.

4. Let $G = \langle a \rangle$ be cyclic.

   Let $x \in G'$ be any element. Since φ is onto, there exists some $t \in G$ such that $\varphi(t) = x$.

   Now $t \in G = \langle a \rangle$. So, $t = a^m$ for some m.

   Therefore $x = \varphi(a^m) = (\varphi(a))^m$.

   Thus any element of G' is some power of $\varphi(a)$.

   Hence $G' = \langle \varphi(a) \rangle$. Therefore, G' is cyclic.

   Similarly, it can be shown that if G' is cyclic, then G is also cyclic.

Remark: In view of the above theorem, in order to show that two groups are not isomorphic, it is enough to show that one group has some structural property, which the other group does not possess.

For example, the groups S_3 and Z_6 are not isomorphic as Z_6 is abelian, whereas S_3 is non-abelian.

Problem 7.10 Show that the groups $U(8)$ and $U(10)$ are not isomorphic.

Solution We have $U(8) = \{1, 3, 5, 7\}$ and $U(10) = \{1, 3, 7, 9\}$.

$U(8)$ and $U(10)$ are both finite groups of order 4.

On computing the orders of the elements of $U(8)$ and $U(10)$, we see that $U(8)$ has three elements of order 2, namely, 3, 5 and 7. But $U(10)$ has only one element of order 2, namely 9. Hence, $U(8)$ and $U(10)$ are not isomorphic.

(If $\varphi : G \to G'$ is an isomorphism, then G and G' have the same number of elements of a given order k.)

Problem 7.11 Show that the groups $U(8)$ and $U(12)$ are isomorphic.

Solution We have $G = U(8) = \{1, 3, 5, 7\}$ and $G' = U(12) = \{1, 5, 7, 11\}$.

Define $\varphi : G \to G'$ by $\varphi(1) = 1$, $\varphi(3) = 5$, $\varphi(5) = 7$, $\varphi(7) = 11$.

Clearly, φ is well defined, one-one and onto.

The multiplication tables of G and G' are

Table 7.1: Multiplication Table for G

$\otimes_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Table 7.2: Multiplication Table for G'

$\otimes_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

From the multiplication table it is clear that

$\varphi(a \otimes_8 b) = \varphi(a) \otimes_{12} \varphi(b)$ for all $a, b \in G$. Hence, $U(8) \cong U(12)$.

Problem 7.12 Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.

Solution We have $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

and $U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$.

Both $U(20)$ and $U(24)$ are abelian groups of order 8.

The order of every element of $U(24)$ other than identity is 2. Thus, $U(24)$ has 7 elements of order 2. In $U(20)$ only three elements, namely 9, 11 and 19 are of order 2. Thus, $U(20)$ and $U(24)$ are not isomorphic.

Problem 7.13 Prove that $\mathbb{Q}$ under addition is not isomorphic to $\mathbb{R}^+$ under multiplication.

Solution Suppose f is an isomorphism from $\mathbb{Q}$ to $\mathbb{R}^+$. Let $f(1) = a$.

For any positive integer m,

$$f(m) = f\underbrace{(1+1+\ldots+1)}_{m \text{ times}}$$

$$= \underbrace{f(1)\cdot f(1)\cdot \ldots \cdot f(1)}_{m \text{ times}} = \underbrace{a\cdot a \ldots a}_{m \text{ times}} = a^m$$

For any negative integer m, $m = -n$, where n is a positive integer.

$$f(m) = f(-n) = (f(n))^{-1} = (a^n)^{-1} = a^{-n} = a^m$$

(As f is an isomorphism, inverse maps to inverse)

Also $f(0) = 1 = a^0$, as in an isomorphism identity is mapped to identity.

Thus $f(a) = a^n$, for all $n \in \mathbb{Z}$

Let $\frac{m}{n} \in \mathbb{Q}$. Now $m = n\left(\frac{m}{n}\right)$. Then $f(m) = f\left(n\left(\frac{m}{n}\right)\right)$

Thus $a^m = f\left(\underbrace{\frac{m}{n}+\frac{m}{n}+\ldots+\frac{m}{n}}_{n \text{ times}}\right) = \left(f\left(\frac{m}{n}\right)\right)^n$,

Hence $f\left(\frac{m}{n}\right) = a^{\frac{m}{n}}$.

Thus f is the mapping defined as $f\left(\frac{m}{n}\right) = a^{\frac{m}{n}}$, for all $\frac{m}{n} \in Q$.

Now $a^\pi \in \mathbb{R}^+$, but there is no rational number $\frac{m}{n}$ such that $f\left(\frac{m}{n}\right) = a^{\frac{m}{n}} = a^\pi$.

Therefore f is not an isomorphism.

Therefore $\mathbb{Q}$ under addition is not isomorphic to $\mathbb{R}^+$ under multiplication.

PROBLEM 7.14 Prove that a group G is abelian if and only if the mapping $f : G \to G$ given by $f(x) = x^2$ is a homomorphism.

SOLUTION Suppose G is abelian. Then $(xy)^2 = x^2y^2 \ \forall\ x, y \in G$

Let $x, y \in G$. Then, $f(xy) = (xy)^2 = x^2y^2 = f(x)\, f(y)$.

Thus f is a homomorphism.

Conversely let the mapping $f : G \to G$ given by $f(x) = x^2$ be a homomorphism.

Then $f(xy) = f(x)f(y) \quad \forall\ x, y \in G$

$\Rightarrow \quad (xy)^2 = x^2\, y^2 \quad \forall\ x, y \in G$

$\Rightarrow \quad xyxy = xxyy$

$\Rightarrow \quad yx = xy \quad \forall\ x, y \in G$ (Using cancellation laws in G)

Hence G is abelian.

PROBLEM 7.15 Prove that a group G is abelian if and only if the mapping $f : G \to G$, given by $f(x) = x^{-1}$, is a homomorphism.

SOLUTION Let the mapping $f : G \to G$ given by $f(x) = x^{-1}$ be a homomorphism.

Let $x, y \in G$ be arbitrary.

We have $f(xy) = f(x)f(y)$ or $(xy)^{-1} = x^{-1}\, y^{-1}$

Premultiplying by xy on both sides, we get

$$e = (xy)x^{-1}y^{-1} \Rightarrow ey = (xy)\, x^{-1} \Rightarrow yx = xy, \forall x, y \in G$$

Hence G is abelian.

Conversely, let G be abelian. Let $x, y \in G$ be arbitrary.

Then $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$, (since G is abelian)

$$= f(x)\, f(y)$$

Hence f is a homomorphism.

PROBLEM 7.16 Show that a homomorphism from a simple group is either trivial or one-one.

SOLUTION Let G be a simple group and f be a homomorphism of G into another group G'.

Then $\ker f$ is a normal subgroup of G.

But the only normal subgroups of the simple group G are $\{e\}$ and G itself.

Therefore either $\ker f = G$ or $\ker f = \{e\}$.

If $\ker f = G$, the f-image of each element of G is the identity of G' and so the homomorphism f is a trivial one.

If $\ker f = \{e\}$, the homomorphism f is one-one.

Hence the result.

Problem 7.17 Let f be a homomorphism of a group G onto another group G' and g, a homomorphism of G' onto G''. Show that the composite mapping $g \circ f$ is a homomorphism of G onto G''. Also show that the ker f is a subgroup of the kernel of $g \circ f$.

Solution Since f is a mapping from G onto G' and g is a mapping from G' onto G'', therefore $g \circ f$ is a mapping from G onto G'' such that

$$(g \circ f)\ (x) = g(f(x)),\ \ \forall\ x \in G$$

Let $a, b \in G$. Then

$$\begin{aligned}(g \circ f)(ab) &= g(f(ab)) \\ &= g(f(a)f(b)) && \text{(as } f \text{ is a homomorphism)} \\ &= g(f(a))g(f(b)) && \text{(as } g \text{ is a homomorphism)} \\ &= (g \circ f)(a)(g \circ f)(b)\end{aligned}$$

Therefore $g \circ f$ is a homomorphism of G onto G''

Let K be the kernel of $g \circ f$.

Then $K = \{y \in G : (g \circ f)(y) = e''\}$, where e'' is the identity of G''.

Let K' be the kernel of f.

Then $K' = \{z \in G : f(z) = e'\}$, where e' is the identity of G'

Both K and K' are normal subgroups of G.

In order to show that K' is a subgroup of K, it is enough to show that $K' \subseteq K$.

Let $k' \in K'$. Then, $f(k') = e'$.

Also $(g \circ f)\,(k') = g(f(k')) = g(e') = e''$.

Therefore $k' \in K$. Thus $K' \subseteq K$.

Exercises

1. Let G be a group of permutations. For each σ in G, define

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is an even permutation} \\ -1 & \text{if } \sigma \text{ is an odd permutation} \end{cases}$$

Prove that sgn is a homomorphism from G to the multiplicative group $\{1, -1\}$. What is the kernel?

2. Let $\mathbb{C}$ be the set of complex numbers with $M = \left\{\begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R}\right\}$. Prove that $\mathbb{C}$ and M are isomorphic under addition and that $\mathbb{C}^*$ and M^*, the non-zero elements of $\mathbb{C}$ and M are isomorphic under multiplication.

3. Let $G = \{a + b\sqrt{2} : a, b \text{ rationals}\}$ and $H = \left\{\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a, b \text{ rationals}\right\}$. Show that G and H are isomorphic under addition. Also, prove that G and H are closed under multiplication.

4. Prove that $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.

5. Let φ be a homomorphism from $U(30)$ to $U(30)$ such that $\varphi(7) = 7$ and $\ker \varphi = \{1, 11\}$. Find all x such that $\varphi(x) = 7$.

6. Let G be the group of real numbers under addition. Show that the mapping $f : G \to G$ defined by $f(x) = [x]$, the greatest integer less than or equal to x, is not a group homomorphism.

7. Show that $U(10)$ is isomorphic to $U(5)$.

8. Determine all homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{10}$. How many of them are onto?

9. Determine all homomorphisms from $\mathbb{Z}_n$ to itself.

10. Let G be a subgroup of some Dihedral group. For each $x \in G$, define

$$\varphi(x) = \begin{cases} +1 & \text{if } x \text{ is a rotation} \\ -1 & \text{if } x \text{ is a reflection} \end{cases}$$

Prove that φ is a homomorphism from the group G to the multiplicative group $\{1, -1\}$. What is the kernel of φ.

Hints to Selected Problems

2. Define $\varphi : \mathbb{C} \to M$, as $\varphi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}, \forall a, b \in \mathbb{R}$.

4. $(\mathbb{Z}, +)$ is a cyclic group, whereas $(\mathbb{Q}, +)$ is not cyclic.

5. We shall use the result:

If $\varphi(g) = g'$, then $\varphi^{-1}(g') = \{x \in G : \varphi(x) = g'\} = g \ker \varphi$

Here, $g' = 7$ and $g = 7$

$U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$, $\ker \varphi = \{1, 11\}$

10. $\ker\varphi$ = set of all rotations in G.

❑❑❑

Check for updates

8

Automorphisms

Learning Objectives

- Definition and Examples of Automorphism of a Group
- Theorems Based on Automorphism of a Group
- Inner Automorphisms

8.1 Automorphism of a Group

We examine a unique type of isomorphism from a group onto itself, as it is imperative in understanding the complexity of many algebraic structures. An automorphism on a structure describes a *symmetry* on that structure—a way in which certain elements of the structure play identical roles within the structure.

Definition 8.1: An isomorphism from a group G onto itself is called an **automorphism of G**, i.e., a mapping from a group G to itself, $f : G \to G$, which is a one-one, onto, homomorphism, is called an automorphism of G.

For example:

1. The identity map from group G onto itself, $I : G \to G$ is an automorphism of G. It is called **trivial automorphism.**
2. Let $\varphi : \mathbb{C} \to \mathbb{C}$ such that $\varphi(a + ib) = a - ib$. Then it can be verified that φ is one−one, onto and homomorphism. Hence, φ is an automorphism on $\mathbb{C}$ under addition.

   Also, the mapping $\theta : \mathbb{C}^* \to \mathbb{C}^*$ defined by $\theta(a + ib) = a - ib$ is an automorphism of the group of non-zero complex numbers under multiplication.
3. The mapping $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, defined by $\varphi(x) = 2x$, $\forall\ x \in \mathbb{Z}$, is not an automorphism, as the mapping is not onto.

© The Author(s) 2023
D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_8

4. Define $\theta : \mathbb{R}^2 \to \mathbb{R}^2$ by $\theta(a, b) = (b, a)$. Then θ is an automorphism of $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ under operation of component-wise addition defined as $(x, y) + (u, v) = (x + u, y + v)$.

   The set of all automorphisms of a group G is denoted by **Aut(G)**.

Theorem 8.1: For any group G, Aut(G) forms a group with respect to composition of mappings.

Proof: Consider the mapping $I : G \to G$, such that $I(x) = x$, $\forall\ x \in G$.

Clearly, I is an isomorphism on G. Therefore, $I \in \text{Aut}(G)$ and hence Aut(G) is non-empty.

Closure: Let $f, g \in \text{Aut}(G)$, then $f : G \to G$ and $g : G \to G$ are automorphisms.

Clearly, $f \circ g : G \to G$ such that $(f \circ g)(x) = f(g(x))$

We now show that $f \circ g$ is an automorphism.

Well defined: Let $x = y$

$\Rightarrow$ $g(x) = g(y)$ ($\because$ g is well defined)

$\Rightarrow$ $f(g(x)) = f(g(y))$ ($\because$ f is well defined)

$\Rightarrow$ $(f \circ g)(x) = (f \circ g)(y)$

Thus, $f \circ g$ is well defined

One-one: Let $(f \circ g)(x) = (f \circ g)(y)$

$\Rightarrow$ $f(g(x)) = f(g(y))$

$\Rightarrow$ $g(x) = g(y)$ ($\because$ f is one $-$one)

$\Rightarrow$ $x = y$ ($\because$ g is one$-$one)

Onto: Let $z \in G$. Since f is onto, there exists some $x \in G$ such that $f(x) = z$. Also, $x \in G$ and g is onto, thus there exists $y \in G$ such that $g(y) = x$.

Therefore we have $f(g(y)) = f(x) = z$. Hence, $f \circ g$ is onto.

Homomorphism:

To show that $(f \circ g)(xy) = (f \circ g)(x)\ (f \circ g)(y)$

Now $(f \circ g)(xy) = f(g(xy))$

$= f(g(x)g(y))$ (since g is homomorphism)

$= (f \circ g)(x) \cdot (f \circ g)(y)$ (since f is homomorphism)

Hence $f \circ g \in \text{Aut}(G)$ and so the closure property holds.

Associativity: To show:

$$(f \circ g) \circ h = f \circ (g \circ h)$$

For all $x \in G$, consider

$$[(f \circ g) \circ h](x) = (f \circ g)\,[h(x)]$$
$$= f[g(h(x))]$$

Also $$[(f \circ (g \circ h)](x) = f[(g \circ h)\,(x)] = f[g(h(x))]$$

So associativity holds true.

Existence of Identity:

To show that $f \circ I = I \circ f = f$, $\forall f \in \text{Aut}(G)$.

We have for all $x \in G$,

$$(f \circ I)\,(x) = f(I(x)) = f(x) \text{ and } (I \circ f)\,(x) = I(f(x)) = f(x)$$

Thus $f \circ I = I \circ f, f \in \text{Aut}(G)$

Existence of inverse: Let $f \in \text{Aut}(G)$. Then f is a bijection.

We need to show that there exists some $f^{-1} \in \text{Aut}(G)$ such that

$$f \circ f^{-1} = f^{-1} \circ f = I.$$

As f is one–one and onto, therefore, $f^{-1} : G \to G$ exists and is also one–one and onto.

Now we show $$f^{-1}(xy) = f^{-1}(x) \cdot f^{-1}(y), \quad \forall\, x, y \in G$$

Let $f^{-1}(x) = u$ and $f^{-1}(y) = v$. Then $x = f(u)$ and $y = f(v)$.

Thus $xy = f(u)\, f(v) = f(uv)$ (since f is homomorphism)

So $f^{-1}(xy) = uv = f^{-1}(x) \cdot f^{-1}(y)$

Therefore $f^{-1} \in \text{Aut}(G)$ and clearly $f \circ f^{-1} = f^{-1} \circ f = I$.

Thus $\text{Aut}(G)$ is a group with respect to composition of functions.

Problem 8.1 Show that $f : G \to G$ such that $f(x) = x^{-1}$ is an automorphism if and only if G is Abelian.

Solution Suppose G is abelian. To show that f is an automorphism.

We have for $x, y \in G$, $x = y$

$\Leftrightarrow$ $x^{-1} = y^{-1}$

$\Leftrightarrow$ $f(x) = f(y)$

Thus f is well defined and one –one.

Clearly, f is onto as for $x \in G$, there exists $x^{-1} \in G$ such that $f(x^{-1}) = (x^{-1})^{-1} = x$

Also $$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} \qquad (\because G \text{ is Abelian})$$
$$= f(x)\, f(y)$$

Therefore f is homomorphism.

Hence $f : G \to G$ is an automorphism.

Conversely let $f : G \to G$ be an automorphism.

Then, $f(xy) = f(x)\, f(y) \quad \forall\ x, y \in G$

This gives $(xy)^{-1} = x^{-1}\, y^{-1}$.

Thus $y^{-1}\, x^{-1} = x^{-1}\, y^{-1}$ and so $xy = yx$, for all $x, y \in G$.
Therefore G is abelian.

Problem 8.2 Let $G = SL(2, \mathbb{R})$ be the group of all 2 by 2 real matrices with determinant 1. Let $A \in G$. Show that the mapping $\varphi_A : G \to G$ defined by $\varphi_A(M) = AMA^{-1}$ is an automorphism.

Solution Since $A, M \in G$, we have AMA^{-1} is a 2 by 2 matrix with real entries and $\det(AMA^{-1}) = \det(A) \cdot \det(M) \cdot (\det(A))^{-1} = 1$. So $AMA^{-1} \in G$ and the mapping is well defined.

Also $\varphi_A(M) = \varphi_A(N)$ gives $AMA^{-1} = ANA^{-1}$ which in turn gives $M = N$. So φ_A is one–one.

Let $N \in G$. To show that there exists some $M \in G$ such that $\varphi_A(M) = N$. Now $\varphi_A(M) = N$ implies $AMA^{-1} = N$. This gives $M = A^{-1}NA$.

Thus $\varphi_A(A^{-1}NA) = A(A^{-1}NA)A^{-1} = N$ and hence φ_A is onto.

Also for all $M, N \in G$, we have

$$\varphi_A(MN) = A(MN)A^{-1} = AM(A^{-1}A)NA^{-1} = (AMA^{-1})\ (ANA^{-1}) = \varphi_A(M)\ \varphi_A(N)$$

Thus φ_A is a homomorphism and hence an automorphism.

8.2 Inner Automorphisms

We now define a special class of automorphism called Inner Automorphism, which can be obtained through simple operations from within the group itself.

Theorem 8.2: If a be any fixed element of a group G, then the mapping $\varphi_a : G \to G$ defined by $\varphi_a(x) = axa^{-1}$, for all $x \in G$ is an automorphism of G.

Proof: Let x, y be any two arbitrary elements of G.

Then $x = y$ if and only if $axa^{-1} = aya^{-1}$ if and only if $\varphi_a(x) = \varphi_a(y)$

Hence φ_a is well defined and one–one.

Now let $g \in G$

Then there exists some $x = a^{-1}\, ga \in G$ such that

$$\varphi_a(a^{-1}\, ga) = a(a^{-1}ga)a^{-1} = g.$$

Therefore, φ_a is onto.

Also $\varphi_a(xy) = a(xy)a^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})\ (aya^{-1}) = \varphi_a(x)\ \varphi_a(y)$

Thus φ_a is homomorphism and hence an automorphism.

This class of automorphisms is very important and is called **inner automorphism** as defined below:

Definition 8.2: Let G be a group and let $a \in G$. The function φ_a defined by $\varphi_a(x) = axa^{-1}$, for all $x \in G$ is called the **inner automorphism of G induced by 'a'.**

Note that for any group G,

Aut(G) = set of all automorphisms on G.

Inn(G) = set of all inner automorphisms on G

Clearly, $\text{Inn}(G) \subseteq \text{Aut}(G)$.

Theorem 8.3: For any group G, the set of all inner automorphisms on G, $\text{Inn}(G)$ is a group.

Proof: Clearly, $\text{Inn}(G) \subseteq \text{Aut}(G)$. So we show $\text{Inn}(G) \leq \text{Aut}(G)$.

Consider $\varphi_e : G \to G$ such that $\varphi_e(x) = exe^{-1} = x$, i.e., $I(x) = \varphi_e(x)$. Since $\varphi_e \in \text{Inn}(G)$, therefore $\text{Inn}(G) \neq \phi$

Closure: Let $\varphi_a, \varphi_b \in \text{Inn}(G)$.

Then $\varphi_a : G \to G$ such that $\varphi_a(g) = aga^{-1}$

and $\varphi_b : G \to G$ such that $\varphi_b(g) = bgb^{-1}$.

Consider $(\varphi_a \circ \varphi_b)(g) = \varphi_a\,(\varphi_b(g)) = \varphi_a(bgb^{-1}) = a(bgb^{-1})a^{-1}$

$= (ab)g\,(b^{-1}a^{-1})$

$= (ab)g\,(ab)^{-1} = \varphi_{ab}(g)$

Thus $\varphi_a \circ \varphi_b = \varphi_{ab} \in \text{Inn}(G)$

Inverse: Let $\varphi_a \in \text{Inn}\,(G)$. To show that $(\varphi_a)^{-1} \in \text{Inn}(G)$

Since $a \in G$ and G is a group, so a^{-1} exists

Consider $\varphi_{a^{-1}} : G \to G$ such that $\varphi_{a^{-1}}(g) = a^{-1}ga$

Clearly, $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{aa^{-1}} = \varphi_e = I$. Similarly, $\varphi_{a^{-1}} \circ \varphi_a = I$.

Since $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a^{-1}} \circ \varphi_a = I$, therefore $(\varphi_a)^{-1} = \varphi_{a^{-1}} \in \text{Inn}(G)$.

Therefore $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$ and hence $\text{Inn}(G)$ is a group.

Problem 8.3 Prove that for any group G, $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

Solution Let $g \in \text{Aut}(G)$ and $f_a \in \text{Inn}(G)$ be arbitrary elements.

Then to show that $gf_ag^{-1} \in \text{Inn}(G)$

We have $(gf_ag^{-1})(x) = gf_a(g^{-1}(x)) = (gf_a)(y)$, where $y = g^{-1}(x)$

$= g(f_a(y)) = g(aya^{-1})$

$= g(a)\,g(y)\,g(a^{-1})$ ($\because$ g is homomorphism)

$= g(a)\ x(g(a))^{-1}$

$= bxb^{-1} = f_b(x),\ \forall\ x \in G,$ where $g(a) = b$

Therefore $g\, f_a g^{-1} = f_b \in \text{Inn}(G)$.

Hence $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

Problem 8.4 Let G be a group, H a subgroup of G, T an automorphism of G. Prove that $T(H) = \{T(h) : h \in H\}$ is a subgroup of G.

Further show that if H is a normal subgroup of G, then $T(H)$ is also a normal subgroup of G.

Solution Since $e \in H$, we have $T(e) \in T(H)$, therefore $T(H)$ is non-empty.

Let $a, b \in T(H)$. Then $a = T(h_1)$, $b = T(h_2)$ for some $h_1, h_2 \in H$.

We have $ab^{-1} = T(h_1)\ (T(h_2))^{-1} = T(h_1)\ T(h_2^{-1})$

$= T(h_1h_2^{-1})$, since T is a homomorphism

Now H is a subgroup of G, so $h_1h_2^{-1} \in H$. Thus, $T(h_1h_2^{-1}) \in T(H)$.

Therefore $ab^{-1} \in T(H)\ \ \forall\ a, b \in T(H)$. Hence, $T(H)$ is a subgroup of G.

We now show that if H is a normal subgroup of G then $T(H)$ is a normal subgroup of G.

Let $g \in G$ and $n \in T(H)$. Then $n = T(h)$ for some $h \in H$.

Since $T : G \to G$ is onto, therefore for $g \in G$, there exists some $g_1 \in G$ such that $T(g_1) = g$.

Then $gng^{-1} = T(g_1)T(h)(T(g_1))^{-1} = T(g_1h)T(g_1^{-1}) = T(g_1hg_1^{-1})$, since T is a homomorphism.

Since H is a normal subgroup of G, therefore $g_1hg_1^{-1} \in H$.

So, $T(g_1hg_1^{-1}) \in T(H)$.

Therefore $gng^{-1} \in T(H),\ \ \forall\ g \in G$ and $n \in T(H)$.

Hence $T(H)$ is a normal subgroup of G.

8.3 Theorems Based on Automorphism of a Group

Theorem 8.4: For any group G, $\dfrac{G}{Z(G)} \cong \text{Inn}(G)$,

Proof: Define a mapping $\theta : G \to \text{Inn}(G)$ by $\theta(a) = f_a$,

where $f_a(x) = axa^{-1},\ \forall\ x \in G$.

Then $a = b$ gives $ax = bx$ implying $axa^{-1} = bxb^{-1}$.

This gives $f_a(x) = f_b(x)$. Thus, $\theta(a) = \theta(b)$.

Hence θ is well defined.

Clearly θ is onto, as for any $f_a \in \text{Inn}(G)$, there exists $a \in G$ such that $\theta(a) = f_a$.

Also $f_{ab}(x) = (ab)x(ab)^{-1} = (ab)x(b^{-1}a^{-1}) = a(bxb^{-1})a^{-1} = f_a(f_b(x))$

Therefore $\theta(ab) = f_{ab} = f_a f_b = \theta(a)\theta(b)$

Thus θ is an onto homomorphism.

Therefore by Theorem 7.6, we have $\text{Inn}(G) \cong \dfrac{G}{\ker \theta}$

Now $a \in \ker \theta \Leftrightarrow \theta(a) = f_e \Leftrightarrow f_a = f_e \Leftrightarrow f_a(x) = f_e(x), \forall\, x \in G$

$\Leftrightarrow axa^{-1} = x, \forall\, x \in G \Leftrightarrow ax = xa, \forall\, x \in G \Leftrightarrow a \in Z(G)$

Thus $\ker \theta = Z(G)$. Hence $\text{Inn}(G) \cong \dfrac{G}{Z(G)}$.

Problem 8.5 Prove that, if for any group G, $\text{Aut}(G)$ is cyclic, then G is abelian.

Solution Let $\text{Aut}(G)$ be cyclic. Then $\text{Inn}(G)$ is cyclic as $\text{Inn}(G) \leq \text{Aut}(G)$.

By Theorem 8.4, we have $\dfrac{G}{Z(G)}$ is cyclic. Therefore G is abelian.

Theorem 8.5: Let G be a group and let H be a subgroup of G, then there exists an isomorphism between $\dfrac{N_G(H)}{C_G(H)}$ and a subgroup of $\text{Aut}(H)$.

Proof: Define a mapping $\varphi : N_G(H) \to \text{Aut}(H)$ by $\varphi(a) = f_a$.

where $f_a : H \to H$ is an inner automorphism such that $f_a(x) = axa^{-1}$.

For $a, b \in N_G(H)$,

$$a = b \Rightarrow ax = bx \Rightarrow axa^{-1} = bxb^{-1} \Rightarrow f_a(x) = f_b(x), \forall x$$

Thus $\varphi(a) = \varphi(b)$. Hence φ is well defined.

Also $\varphi(ab) = f_{ab} = f_a f_b = \varphi(a)\varphi(b)$. Thus φ is a homomorphism.

Now $a \in \ker \varphi \Leftrightarrow \varphi(a) = f_e \Leftrightarrow f_a = f_e \Leftrightarrow f_a(x) = f_e(x)\ \forall\ x \in H$ $\Leftrightarrow axa^{-1} = x, \forall\, x \in H \Leftrightarrow ax = xa, \forall\, x \in H \Leftrightarrow a \in C_G(H)$

Therefore $\ker \varphi = C_G(H)$.

But φ is not onto. Therefore we cannot apply Theorem 7.6.

So we have to restrict to co-domain $\varphi(N_G(H))$.

If $\varphi : N_G(H) \to \varphi(N_G(H))$, then it becomes onto. Therefore, by Theorem 7.6,

$$\frac{N_G(H)}{C_G(H)} \cong \text{subgroup of } \text{Aut}(H)$$

(since $\varphi(N_G(H))$ is a subgroup of $\text{Aut}(H)$)

Problem 8.6 Let G be a group and Z the centre of G. If T is any automorphism of G, prove that $T(Z) \subseteq Z$.

Solution We know $Z = \{a \in G : ag = ga \ \forall \ g \in G\}$ and $T(Z) = \{T(a) : a \in Z\}$.

Let $y \in T(Z)$, then $y = T(a)$ for some $a \in Z$. ...(1)

Now $a \in Z$ implies $ag = ga \ \forall \ g \in G$ ...(2)

Since $T : G \to G$ is onto, therefore for any $g \in G$, there exists some $g_1 \in G$ such that $T(g_1) = g$. ...(3)

We have
$$\begin{aligned} yg &= T(a)\ T(g_1) && \text{(using (1) and (3))} \\ &= T(ag_1) && \text{(since } T \text{ is a homomorphism)} \\ &= T(g_1 a) && \text{(from (2))} \\ &= T(g_1)\ T(a) && \text{(since } T \text{ is a homomorphism)} \\ &= gy && \text{(using (1) and (3))} \end{aligned}$$

$\therefore \quad yg = gy \quad \forall \ g \in G$

Thus $y \in Z$ for each $y \in T(Z)$. Hence, $T(Z) \subseteq Z$.

Problem 8.7 Let $f : G \to G$ defined as $f(a) = a^n$ be an automorphism. Show that $a^{n-1} \in Z(G)$ for all $a \in G$.

Solution Let $a, x \in G$. Then $f(a^{-n}\, xa^n) = (a^{-n}\, xa^n)^n$

$$= \underbrace{(a^{-n}\, xa^n)(a^{-n} xa^n) \ldots (a^{-n} xa^n)}_{n \text{ times}}$$

$$= a^{-n}(xx \ldots x)a^n \qquad \text{(since } a^n\, a^{-n} = e\text{)}$$

$$= a^{-n}\, x^n a^n$$

$$= f(a^{-1}) f(x) f(a),$$

Therefore $f(a^{-n}\, xa^n) = f(a^{-1} xa)$, since f is a homomorphism

Thus $a^{-n}\, xa^n = a^{-1}\, xa$, since f is one to one.

On premultiplying by a^n and post-multiplying by a^{-1}, we get

$xa^{n-1} = a^{n-1}x$ for all $a, x \in G$. Hence $a^{n-1} \in Z(G)$ for all $a \in G$.

Problem 8.8 Find Aut(G), where G, generated by a, is any infinite cyclic group.

Or

If G is an infinite cyclic group, then show that Aut(G) is isomorphic to a cyclic group of order 2.

Solution Let $G = \langle a \rangle$ and let $f \in \text{Aut}(G)$ be any member.

Then $f : G \to G$ is an automorphism.

Let $x \in G$ be any element. Since f is onto, there exists some $y \in G$ such that $x = f(y)$.

Now $y \in G = \langle a \rangle$ implies $y = a^k$.

Therefore $x = f(y) = f(a^k) = (f(a))^k$ ($\because f$ is homomorphism)

Thus $G = \langle f(a) \rangle$.

Since an infinite cyclic group has two generators a and a^{-1}, therefore f has only two choices.

One of these is the identity map and other is defined by $\theta(x) = x^{-1}$.

Now G being cyclic, is abelian and so θ is an automorphism.

Also, $\theta \neq I$ as if $\theta = I$, then $\theta(a) = I(a)$

$\Rightarrow \quad a^{-1} = a$

$\Rightarrow \quad a^2 = e$

Thus $o(a) \leq 2$ which is finite, a contradiction, as $o(a) = o(G)$ is infinite.

So $\theta \neq I$. Hence $o(\text{Aut}(G)) = 2$, a prime number and

$$\text{Aut}(G) = \{I, \theta : \theta(x) = x^{-1}\}$$

Since $\text{Aut}(G)$ is a cyclic group of order 2 and any cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Therefore, $\text{Aut}(G)$ is isomorphic to $\mathbb{Z}_2$.

Problem 8.9 Find $\text{Aut}(\mathbb{Z})$, where $\mathbb{Z}$ is the group of integers under addition.

Solution Since $\mathbb{Z}$ is an infinite cyclic group, so by problem 8.8, we have

$$\text{Aut}(\mathbb{Z}) = \{I, \theta : \theta(x) = -x\}.$$

Since it is a cyclic group of order 2, it is isomorphic to $\mathbb{Z}_2$.

Problem 8.10 Find $\text{Aut}(G)$ where $G = \langle a \rangle$ is a finite cyclic group of order n.

Solution Let $f \in \text{Aut}(G)$ be any member. Then $f : G \to G$ is an onto homomorphism.

Let $x \in G$ then there exists some $y \in G$ such that $x = f(y)$.

Since $y \in G = \langle a \rangle$, so $y = a^r$ for some r.

Thus $x = f(a^r) = (f(a))^r$ (since f is homomorphism)

Hence $G = \langle f(a) \rangle$.

Since the number of generators of a finite cyclic group of order n is $\varphi(n)$, so G has $\varphi(n)$ generators. Therefore, f has $\varphi(n)$ choices.

Define $f_m : G \to G$ such that $f_m(x) = x^m$, where $1 \le m < n$, and $\gcd(m, n) = 1$.

Let $x = y$ then $x^m = y^m$ implies $f_m(x) = f_m(y)$ and so f_m is well defined.

Now $f_m(x) = f_m(y)$ gives $x^m = y^m$ implying $x^m y^{-m} = e$.

Thus $(xy^{-1})^m = e$, so $o(xy^{-1}) \mid m$.

Also $o(xy^{-1}) \mid n$ (since if $a \in G$ then $o(a) \mid o(G)$)

Therefore $o(xy^{-1}) = 1$ as $\gcd(m, n) = 1$.

This gives $xy^{-1} = e$ and so $x = y$. Hence f_m is one–one.

Also $f_m(xy) = (xy)^m = x^m y^m = f_m(x) f_m(y)$.

Thus f_m is homomorphism.

As G is finite and f_m is one–one, we have f_m is onto also.

Hence f_m is an automorphism.

Now there are $\varphi(n)$ automorphisms. We now show that no two of them are equal.

Suppose $f_r = f_s$, where $1 \le r, s < n$, $\gcd(r, n) = 1$, $\gcd(s, n) = 1$

Then $f_r(a) = f_s(a)$ implies $a^r = a^s$.

Assuming $r > s$, we have $a^{r-s} = e$.

Thus $o(a) \mid r - s$ and therefore $n \mid r - s$.

Therefore $n \le r - s < n$, i.e, $n < n$, a contradiction.

Hence there are precisely $\varphi(n)$ number of automorphisms.

Thus $\text{Aut}(G) = \{f_m : f_m(x) = x^m, 1 \le m < n, \gcd(m, n) = 1\}$.

Theorem 8.6: If G is a finite cyclic group of order n, then

$$\text{Aut}(G) \cong U(n)$$

Proof: Define $\theta : \text{Aut}(G) \to U(n)$ by

$$\theta(f_m) = m, \quad 1 \le m < n, \gcd(m, n) = 1$$

(We know that when G is a finite cyclic group of order n, then

$$\text{Aut}(G) = \{f_m : f_m(x) = x^m : 1 \le m < n, \gcd(m, n) = 1\})$$

Then θ is clearly well defined and onto.

Now $\theta(f_r) = \theta(f_s)$ gives $r = s$ implying $x^r = x^s \ \forall x$.

Thus $f_r(x) = f_s(x) \ \forall x$ and so $f_r = f_s$. Therefore θ is one–one.

To show θ is homomorphism, we need to show $\theta(f_r f_s) = \theta(f_r)\ \theta(f_s)$

Now $f_r f_s(x) = f_r(f_s(x)) = f_r(x^s) = (x^s)^r = x^{rs} = f_{rs}(x)$

Therefore $\theta(f_r f_s) = \theta(f_{rs}) = rs = \theta(f_r)\ \theta(f_s)$

(since $r, s < n$, $\gcd(r, n) = 1$, $\gcd(s, n) = 1$, so, $r, s \in U(n)$ and $rs = r \otimes_n s$)

Thus θ is homomorphism and hence θ is an isomorphism.

Therefore $\text{Aut}(G)$ is isomorphic to $U(n)$.

Problem 8.11 Show that $\text{Aut}(Z_n) \cong U(n)$.

Solution Since Z_n is a finite cyclic group of order n therefore by Theorem 8.6, we have $\text{Aut}(Z_n) \cong U(n)$.

Problem 8.12 Show by an example that we can have groups G and H such that $G \ncong H$ but $\text{Aut}(G) \cong \text{Aut}(H)$.

Solution Let $G = Z_3$ and $H = Z_6$. Then $G \ncong H$ as $o(G) \neq o(H)$.

But since G and H are finite cyclic groups, we have

$$\text{Aut}(G) \cong U_3 = \{1, 2\} \quad \text{and} \quad \text{Aut}(H) \cong U_6 = \{1, 5\}.$$

We will now show that $\text{Aut}(G) \cong \text{Aut}(H)$.

Define a map $f : U_3 \to U_6$ by $f(1) = 1,\ f(2) = 5$.

Then clearly f is an isomorphism and hence $U_3 \cong U_6$.

Thus $\text{Aut}(G) \cong \text{Aut}(H)$.

Problem 8.13 Find $\text{Aut}(G)$, if $G = \langle a \rangle$ and $a^{12} = e$.

Solution The positive integers less than 12 and relatively prime to 12 are 1, 5, 7, 11, i.e., $\varphi(12) = 4$.

Therefore, $\text{Aut}(G) = \{I, f_1, f_2, f_3\}$, where

$$I(x) = x, \quad \forall\ x \in G$$
$$f_1(x) = x^5, \quad \forall\ x \in G$$
$$f_2(x) = x^7, \quad \forall\ x \in G$$
$$f_3(x) = x^{11}, \quad \forall\ x \in G$$

Problem 8.14 Determine $\text{Aut}(\mathbb{Z}_{12})$.

Solution Let $f \in \text{Aut}(\mathbb{Z}_{12})$. For any $k \in \mathbb{Z}_{12}$,

$$f(k) = f\underbrace{(1 + 1 + \ldots + 1)}_{k \text{ times}} = f\underbrace{(1) + f(1) + \ldots + f(1)}_{k \text{ times}} = kf(1).$$

Now for all $a \in \mathbb{Z}_{12}$, $o(a) = o(f(a))$. As $o(1) = 12$ in $\mathbb{Z}_{12}$ this gives that $o(f(1)) = 12$ in $\mathbb{Z}_{12}$.

$\Rightarrow$ $\quad f(1) = 1$ or 5 or 7 or 11

Let $\quad f_1 : 1 \mapsto 1, \quad$ i.e., $f_1(1) = 1 \Rightarrow f_1(x) = x \bmod 12$

$f_2 : 1 \mapsto 5, \quad$ i.e., $f_2(1) = 5 \Rightarrow f_2(x) = 5x \bmod 12$

$f_3 : 1 \mapsto 7, \quad$ i.e., $f_3(1) = 7 \Rightarrow f_3(x) = 7x \bmod 12$

$f_4 : 1 \mapsto 11, \quad$ i.e., $f_4(1) = 11 \Rightarrow f_4(x) = 11x \bmod 12$

Let $S = \{f_1, f_2, f_3, f_4\}$. We first see if each of these is an automorphism.

Since f_1 is an identity map, it is an automorphism.

Now consider f_2, we have

$x = y \Rightarrow x \bmod 12 = y \bmod 12 \Rightarrow 5x \bmod 12 = 5y \bmod 12 \Rightarrow f_2(x) = f_2(y)$

This gives that f_2 is well-defined. Also since $f_2(1) = 5$, f_2 is onto.

Since $\mathbb{Z}_{12}$ is finite dimensional, f_2 is one-one also.

Now, $f_2(a \oplus_{12} b) = (5((a + b) \bmod 12)) \bmod 12$

and $f_2(a) \oplus_{12} f_2(b) = (5a \bmod 12) \oplus_{12} (5b \bmod 12) = ((5a \bmod 12) + (5b \bmod 12)) \bmod 12 = (5(a + b) \bmod 12) \bmod 12$.

Thus, $f_2(a \oplus_{12} b) = f_2(a) \oplus_{12} f_2(b)$

Thus $f_2 \in \text{Aut}(\mathbb{Z}_{12})$

Similarly, it can be seen that f_3 and f_4 are automorphisms and hence belong to $\text{Aut}(\mathbb{Z}_{12})$.

Also, $(f_2 f_2)(1) = f_2(f_2(1)) = f_2(5) = 5.5 \bmod 12 = 1 = f_1(1) \Rightarrow f_2 f_2 = f_1$.

The Cayley Table of $\text{Aut}(\mathbb{Z}_{12})$ is given by

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Also, for no $\varphi \in \text{Aut}(\mathbb{Z}_{12})$, $o(\varphi) = o(\text{Aut}(\mathbb{Z}_{12})) = 4$.

So, $\text{Aut}(\mathbb{Z}_{12})$ is non-cyclic.

Since $\text{Aut}(\mathbb{Z}_{12}) \cong U(12)$ and $U(12)$ is abelian, so $\text{Aut}(\mathbb{Z}_{12})$ is abelian.

Problem 8.15 Prove that if G is a group such that $x^2 \neq e$ for some $x \in G$, then G has a non-trivial automorphism.

Solution The identity mapping $I : G \to G$ defined as $I(x) = x$, $\forall\ x \in G$ is a trivial automorphism.

Case I: If G is abelian. Then $T : G \to G$, defined as $T(x) = x^{-1}$, $\forall\ x \in G$ is an automorphism.

Further, $T \neq I$, as if $T = I$ then $T(g) = I(g)$, $\forall\ g \in G$

This implies, $g^{-1} = g$, $\forall\ g \in G$ and so $g^2 = e$, $\forall\ g \in G$, which is contrary to the given hypothesis.

Thus T is a non-trivial automorphism of G, if G is abelian.

Case II: If G is non-abelian.

Then there exists some inner automorphism $T_g \neq I$, $\forall\ g \in G$.

(as, if $T_g = I$, $\forall\ g \in G$, then $T_g(x) = I(x)$, $\forall\ x \in G$

$\Rightarrow \quad gxg^{-1} = x$, $\forall\ g, x \in G \ \Rightarrow\ gx = xg, \ \forall\ g, x \in G$

$\Rightarrow \quad G$ is abelian, which is a contradiction.)

Thus, in any case, G has a non-trivial automorphism.

Problem 8.16 Let G be a group and T an automorphism of G. If N is a normal subgroup of G such that $T(N) \subset N$, show how you could use T to define an automorphism of G/N.

Solution

Define a mapping $\theta : G/N \to G/N$ as $\theta(Ng) = NT(g) \ \ \forall\ g \in G$ ...(1)

Note that $T(g) \in G\ \forall\ g \in G$ and so $NT(g) \in G/N$

We verify that θ is well defined.

Let $Ng_1 = Ng_2 \ \Rightarrow\ g_1g_2^{-1} \in N \ \Rightarrow\ T(g_1g_2^{-1}) \in T(N)$

$\Rightarrow \quad T(g_1g_2^{-1}) \in N$ (As $T(N) \subset N$)

$\Rightarrow \quad T(g_1)\ T(g_2^{-1}) \in N$, (since T is a homomorphism)

$\Rightarrow \quad T(g_1)\ (T(g_2))^{-1} \in N$, (since T is homomorphism)

$\Rightarrow \quad NT(g_1) = NT(g_2)$.

Thus θ is well defined.

Now we show that θ is one to one.

Let $\theta(Ng_1) = \theta(Ng_2)$, $g_1, g_2 \in G$

$\Rightarrow \quad NT(g_1) = NT(g_2)$

$\Rightarrow \quad T(g_1)\ (T(g_2))^{-1} \in N$

$\Rightarrow \quad T(g_1)\ T(g_2^{-1}) \in N$

$\Rightarrow \quad T(g_1g_2^{-1}) \in N$, (since T is homomorphism)

$\Rightarrow \quad g_1g_2^{-1} \in N$ (As $T(N) \subset N$)

$\Rightarrow \quad Ng_1 = Ng_2$

Therefore θ is one to one.

Next we show that θ is onto.

Let $x \in G/N$ so that $x = Ng$ for some $g \in G$.

Since T is onto, there exist some $g' \in G$ such that $T(g') = g$.

Therefore $x = Ng = NT(g') = \theta(Ng')$, (by (1))

Since $Ng' \in G/N$, therefore θ is onto.

Finally, we show that θ is homomorphism.

Let $a = Ng_1, b = Ng_2 \in G/N$.

Then $ab = Ng_1Ng_2 = Ng_1g_2 \in G/N$.

Therefore
$$\begin{aligned}\theta(ab) &= \theta(Ng_1g_2) = NT(g_1g_2)\\ &= N(T(g_1)T(g_2)), \quad \text{(as } T \text{ is homomorphism)}\\ &= NT(g_1)\, NT(g_2), \text{ (as } T(g_1), T(g_2) \in G \text{ and } N \trianglelefteq G)\\ &= \theta(T(g_1))\ \theta(T(g_2))\\ &= \theta(a)\ \theta(b).\end{aligned}$$

Thus θ is homomorphism.

Hence we have used T, as given in (1), to define an automorphism θ of G/N.

Problem 8.17 Determine $\text{Inn}(D_4)$.

Solution We know $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_D, F_{D'}\}$ is a group under function composition. The inner automorphism induced by the elements of D_4 are $\varphi_{R_0}, \varphi_{R_{90}}, \varphi_{R_{180}}, \varphi_{R_{270}}, \varphi_{F_H}, \varphi_{F_V}, \varphi_{F_D}, \varphi_{F_{D'}}$.

We now see which of these are equal.

Since R_{180} commutes with each element of D_4, we have

$$\varphi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = R_{180}xR_{180} = R_{180}R_{180}x = x = \varphi_{R_0}(x)$$

Thus $\varphi_{R_{180}} = \varphi_{R_0}$.

Similarly
$$\begin{aligned}\varphi_{R_{270}}(x) &= R_{270}xR_{270}^{-1} = R_{90}R_{180}x(R_{90}R_{180})^{-1}\\ &= R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1} = \varphi_{R_{90}}(x)\end{aligned}$$

Thus $\varphi_{R_{270}} = \varphi_{R_{90}}$.

Also we have $R_{180}\, F_H = F_V$, therefore

$$\begin{aligned}\varphi_{F_V}(x) = F_VxF_V^{-1} = R_{180}F_Hx(F_HR_{180})^{-1} &= F_HR_{180}xR_{180}F_H^{-1}\\ &= F_HxF_H^{-1} = \varphi_{F_H}(x)\end{aligned}$$

So $\varphi_{F_V} = \varphi_{F_H}$.

In the same way we have since $R_{180}\, F_D = F_{D'}$, thus $\varphi_{F_D} = \varphi_{F_{D'}}$.

Therefore $\text{Inn}(D_4) = \{\varphi_{R_0}, \varphi_{R_{90}}, \varphi_{F_H}, \varphi_{F_D}\}$.

The action induced by R_{90} on elements of D_4 is given by

$$\varphi_{R_{90}}(x) = R_{90}xR_{90}^{-1} = R_{90}xR_{270}\ ,\ x \in D_4$$

Now $\varphi_{R_{90}}(R_0) = R_{90}R_0R_{270} = R_0,\ \varphi_{R_{90}}(R_{90}) = R_{90}R_{90}R_{270} = R_{90},$

$\varphi_{R_{90}}(R_{180}) = R_{90}R_{180}R_{270} = R_{180},\ \varphi_{R_{90}}(R_{270}) = R_{90}R_{270}R_{270} = R_{270},$

$\varphi_{R_{90}}(F_H) = R_{90}F_HR_{270} = F_V,\ \varphi_{R_{90}}(F_V) = R_{90}F_VR_{270} = F_H,$

$\varphi_{R_{90}}(F_D) = R_{90}F_DR_{270} = F_{D'},\ \varphi_{R_{90}}(F_{D'}) = R_{90}F_{D'}R_{270} = F_D.$

Similarly the action induced by F_H on elements of D_4 is given by

$$\varphi_{F_H}(x) = F_HxF_H^{-1} = F_HxF_H,\ x \in D_4$$

Thus $\varphi_{F_H}(R_0) = F_HR_0F_H = R_0,\ \varphi_{F_H}(R_{90}) = F_HR_{90}F_H = R_{270},$

$\varphi_{F_H}(R_{180}) = F_HR_{180}F_H = R_{180},\ \varphi_{F_H}(R_{270}) = F_HR_{270}F_H = R_{90},$

$\varphi_{F_H}(F_H) = F_HF_HF_H = F_H,\ \varphi_{F_H}(F_V) = F_HF_VF_H = F_V,$

$\varphi_{F_H}(F_D) = F_HF_DF_H = F_{D'},\ \varphi_{F_H}(F_{D'}) = F_HF_{D'}F_H = F_D.$

PROBLEM 8.18 Are the following mappings automorphisms of their respective groups?

(a) G group of integers under addition, $T : x \to -x$.

(b) G group of positive real numbers under multiplication, $T : x \to x^2$.

(c) G cyclic group of order 12, $T : x \to x^3$.

(d) G is the group S_3, $T : x \to x^{-1}$

SOLUTION

(a) Yes, as G is an abelian group.

(b) No, as mapping is not a homomorphism.

(c) No, as if $G = \langle a \rangle$, then $o(a) = 12$, while $o(T(a)) = 4$, showing T is not an automorphism. Note that an isomorphism preserve the order of elements.

(d) No, as G is a non-abelian group, so the mapping $T : x \to x^{-1}$ fails to be an automorphism.

PROBLEM 8.19 Let G be a group of order 4, $G = \{e, a, b, ab\}$, $a^2 = b^2 = e$, $ab = ba$. Determine Aut(G).

SOLUTION The possible proper subgroups of G are $\{e, a\}$, $\{e, b\}$, $\{e, ab\}$.

We aim at finding a mapping T which is an automorphism.

Since T is homomorphism, therefore $T(e) = e$.

Also once we have found $T(a)$ and $T(b)$, the value of $T(ab)$ gets decided by itself as $T(ab) = T(a)T(b)$.

Now what could be the possible values of $T(a)$ so that T is an automorphism.

Since $o(a) = 2$, so $o(T(a))$ must be 2.

The elements with order 2 are a, b, ab, so $T(a)$ has three choices namely a, b, ab.

Once $T(a)$ is decided, what could be the possible values for $T(b)$.

Again order of b is 2, so the order of $T(b)$ must be 2.

Again we have three possible candidates, a, b, ab, out of which one has already been fixed to $T(a)$.

So $T(b)$ has two choices. Thus we have $3 \times 2 = 6$ possible automorphisms.

Thus

$$\text{Aut}(G) = \left\{ \begin{bmatrix} e & a & b & ab \\ e & a & b & ab \end{bmatrix}, \begin{bmatrix} e & a & b & ab \\ e & a & ab & b \end{bmatrix}, \begin{bmatrix} e & a & b & ab \\ e & b & a & ab \end{bmatrix}, \begin{bmatrix} e & a & b & ab \\ e & b & ab & a \end{bmatrix}, \begin{bmatrix} e & a & b & ab \\ e & ab & a & b \end{bmatrix}, \begin{bmatrix} e & a & b & ab \\ e & ab & b & a \end{bmatrix} \right\}$$

Problem 8.20 (a) A subgroup C of G is said to be a characteristic subgroup of G if $T(C) \subset C$ for all automorphisms T of G.

Prove that a characteristic subgroup of G must be a normal subgroup of G.

(b) Prove that the converse of (*a*) is false.

Solution

(a) For some $g \in G$, define $T_g : G \to G$ such that $T_g(x) = gxg^{-1}$

It is easy to check that T_g is an automorphism of G for all $g \in G$.

But it is given that $T(C) \subset C$ for all automorphisms T.

So $T_g(C) \subset C$, $\forall\ g \in G$.

But that means $gCg^{-1} \subset C$, or $gcg^{-1} \in C$, $\forall\ g \in G$ and $\forall\ c \in C$.

Thus, C is a normal subgroup of G.

(b) We simply give an example to show that converse of part(a) need not be true.

For $G = \{e, a, b, ab\}$ with $a^2 = e$, $b^2 = e$ and $ab = ba$; and $C = \{e, a\}$; and

$$T = \begin{bmatrix} e & a & b & ab \\ e & b & a & ab \end{bmatrix}.$$

We have C is a normal subgroup of G but $T(C) \not\subseteq C$.

Note that T defined above is an automorphism of G.

Problem 8.21 If G is a group, N a normal subgroup of G, M a characteristic subgroup of N, prove that M is a normal subgroup of G.

Solution Let $g \in G$. We define $T_g : G \to G$ such that $T_g(x) = gxg^{-1}$.

Clearly, T_g is an automorphism of G.

Also $T_g(N) = N$ as N is given to be normal in G.

Now consider $T_g : N \to N$. Since $T_g(N) = N$, one can easily see T_g is an automorphism of N too.

But then $T_g(M) \subset M$ as M is given to be a characteristic subgroup of N.

So $gMg^{-1} \subset M$, $\forall g \in G$, or $gmg^{-1} \in M$, $\forall\ g \in G$ and $\forall m \in M$.

Hence M is normal in G.

Problem 8.22 Let G be a finite group, T an automorphism of G with the property that $T(x) = x$ for $x \in G$ if and only if $x = e$. Prove that every $g \in G$ can be represented as $g = x^{-1}\ T(x)$ for some $x \in G$.

Solution G is given to be a finite group.

We define mapping $\varphi : G \to G$ such that $\varphi(x) = x^{-1}\ T(x)$.

Clearly, the mapping so defined is well defined.

Also $\varphi(a) = \varphi(b) \Rightarrow a^{-1}\ T(a) = b^{-1}T(b) \Rightarrow T(a)(T(b))^{-1} = ab^{-1}$

$\Rightarrow \qquad T(ab^{-1}) = ab^{-1}$.

But $T(x) = x$ implies $x = e$, so $\varphi(a) = \varphi(b)$ implies $ab^{-1} = e$, i.e., $a = b$.

Thus the mapping φ is one-to-one.

But since G is finite, therefore φ being one-to-one implies φ is onto too.

But onto implies that if some $g \in G$, then it has its preimage in G,

i.e., $g = x^{-1}\ T(x)$ for some $x \in G$.

Hence every element g of G can be represented as $x^{-1}\ T(x)$ for some $x \in G$.

Problem 8.23 Let G be a finite group, T an automorphism of G with the property that $T(x) = x$ if and only if $x = e$. Suppose further that $T^2 = I$. Prove that G must be abelian.

Solution Using previous problem, if some $g \in G$, then $g = x^{-1}T(x)$ for some $x \in G$.

So we have $T(g) = T(x^{-1}T(x)) = T(x^{-1})T(\mathrm{T}(x))$

$= (T(x))^{-1}T^2(x) = (T(x))^{-1}\ x$

$= (x^{-1}\ T(x))^{-1} = g^{-1}$.

Thus $T(g) = g^{-1}$, $\forall\ g \in G$.

Now let $a, b \in G$. So we have, $T(ab) = (ab)^{-1} = b^{-1}a^{-1}$ ...(1)

Also $T(ab) = T(a)T(b) = a^{-1}\, b^{-1}$ ...(2)

Using (1) and (2), we have $b^{-1}a^{-1} = a^{-1}b^{-1} \Rightarrow ab = ba$

So we have $ab = ba \ \forall \ a, b \in G$.

Hence G is an abelian group.

Exercises

1. Let $G = \langle a \rangle$ be a finite cyclic group of order n. Show that the mapping $g : a \to a^m$ is an automorphism if and only if m and n are relatively prime.

2. Find Aut(G), if $G = \langle a \rangle$, $a^{10} = e$.

3. Find Aut(G), if $G = \langle a \rangle$, $a^{15} = e$.

4. Compute Aut(G), if $G = \mathbb{Z}_8$.

5. Determine Aut($\mathbb{Z}_{10}$). Is Aut($\mathbb{Z}_{10}$) cyclic?

6. Find the action of inner automorphism of D_4 induced by the element F_D of D_4.

7. Find Inn(D_3).

8. Find Aut($\mathbb{Z}_{14}$).

9. Show that the mapping $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ defined by

$\varphi(a_1, a_2, ..., a_n) = (-a_1, -a_2, ... , -a_n)$ is an automorphism.

10. Find Inn(Q_8).

Hints to Selected Problems

2. Aut(G) = $\{I, f_1, f_2, f_3\}$ where $I(x) = x, f_1 = x^3, f_2(x) = x^7, f_3(x) = x^9$.

4. Aut($\mathbb{Z}_8$) = $\{f_1, f_2, f_3, f_4\}$, where $f_1(x) = x \bmod 8$, $f_2(x) = 3x \bmod 8$, $f_3(x) = 5x \bmod 8$, $f_4(x) = 7x \bmod 8$.

5. Aut($\mathbb{Z}_{10}$) = $\{f_1, f_2, f_3, f_4\}$, where $f_1(x) = x \bmod 10$, $f_2(x) = 3x \bmod 10$, $f_3(x) = 7x \bmod 10$, $f_4(x) = 9x \bmod 10$. Yes, it is cyclic.

10. Inn(Q_8) = $\{g_1, g_i, g_j, g_k\}$, where

$g_1(x) = 1x1^{-1} = x \ \forall \ x \in Q_8$

$g_i(x) = ixi^{-1} = ix(-i) = -ixi \ \forall \ x \in Q_8$

$g_j(x) = -jxj \ \forall \ x \in Q_8$

$g_k(x) = -kxk \ \forall \ x \in Q_8$.

Check for updates

9

Direct Products

Learning Objectives

- External Direct Product
- Internal Direct Product
- Fundamental Theorem of Finite Abelian Groups

In this chapter, we observe direct product of groups, to create new groups from already existing groups. This is a simple technique to combine two groups into a new, larger group. If we understand this mechanism, we can comprehend some large groups more easily. Just as we can factor integers into prime numbers, we can break apart some groups into a direct product of simpler groups. Knowledge of direct products drives significant developments in coding theory and in cryptography.

9.1 External Direct Product

Definition 9.1: Let G_1 and G_2 be two groups. The **external direct product** of G_1, G_2 written as $G_1 \oplus G_2$, is defined as

$$G_1 \oplus G_2 = \{(g_1, g_2) : g_i \in G_i\}$$

where $(g_1, g_2)\,(g_1', g_2') = (g_1 g_1', g_2 g_2')$

It is understood that each product $g_i\, g_i'$ is performed with the operation of G_i.

Definition 9.2: Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The **external direct product** of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \ldots \oplus G_n$, is defined as

$$G_1 \oplus G_2 \oplus \ldots \oplus G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i\}$$

where $(g_1, g_2, \ldots, g_n)\,(g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2\, g_2', \ldots, g_n g_n')$

It is understood that each product $g_i\, g_i'$ is performed with the operation of G_i.

© The Author(s) 2023
D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_9

Thus $G_1 \oplus G_2 \oplus ... \oplus G_n$ is the set of all n–tuples such that the ith component of a tuple is an element of G_i and the operation is component-wise.

Theorem 9.1: Let $G_1, G_2, ... , G_n$ be a finite collection of groups. Then, $G_1 \oplus G_2 \oplus ... \oplus G_n$ forms a group with respect to the composition defined in definition 9.2.

Proof: Let $G_1, G_2, ... , G_n$ be a finite collection of groups. To show that the external direct product $G_1 \oplus G_2 \oplus ... \oplus G_n$ is a group.

Let $G = G_1 \oplus G_2 \oplus ... \oplus G_n$

1. **Closure:** Let $a = (g_1, g_2, ..., g_n)$ and $b = (g_1', g_2', ... , g_n')$ be any two elements of G. Then,

   $ab = (g_1, g_2, ..., g_n)\ (g_1', g_2', ... , g_n') = (g_1g_1', g_2g_2', ... , g_ng_n') \in G$

   Therefore closure holds.

2. **Associativity:** Let $a = (g_1, g_2, ..., g_n)$, $b = (g_1', g_2', ... , g_n')$, $c = (g_1'', g_2'', ... , g_n'') \in G$. Then,

   $$\begin{aligned} a(bc) &= (g_1, g_2, ..., g_n)\ (g_1'g_1'', g_2'g_2'', ... , g_n'g_n'') \\ &= (g_1(g_1'g_1''), g_2(g_2'g_2''), ..., g_n(g_n'g_n'')) \\ &= ((g_1g_1')g_1'', (g_2g_2')g_2'', ..., (g_ng_n')g_n'') \\ &= (g_1g_1', g_2g_2', ..., g_ng_n')\ (g_1'', g_2'', ... ,g_n'') \\ &= (ab)c \end{aligned}$$

3. **Identity:** Let e_i, be the identity element of G_i, for each $i = 1, 2, ... n$.

   Then $e = (e_1, e_2, ... , e_n)$ is the identity element of G.

4. **Inverse:** For every $(g_1, g_2, ..., g_n) \in G$ there exists $(g_1^{-1}, g_2^{-1}, ... , g_n^{-1}) \in G$ such that

   $(g_1, g_2, ..., g_n)\ (g_1^{-1}, g_2^{-1}, ... , g_n^{-1}) = e$

   $= (g_1^{-1}, g_2^{-1}, ... , g_n^{-1})\ (g_1, g_2, ..., g_n)$

   Therefore, $G = G_1 \oplus G_2 \oplus ... \oplus G_n$ forms a group.

Examples:

1. Consider $U(6) \oplus U(8)$. We have

   $U(6) = \{1, 5\} \bmod 6$ and $U(8) = \{1, 3, 5, 7\} \bmod 8$. Then,

   $U(6) \oplus U(8) = \{(a, b) : a \in U(6), b \in U(8)\}$

   $= \{(1, 1), (1, 3), (1, 5), (1, 7), (5, 1)\ (5, 3), (5, 5), (5, 7)\}$

   The product $(5, 3)(1, 7) = (5 \otimes_6 1, 3 \otimes_8 7) = (5, 5)$, here the first two components are combined by multiplication modulo 6, whereas the second two components are combined by multiplication modulo 8. The identity element of this group is (1, 1).

2. Consider $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. Then,

   $$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$$

   Since the operation in each component is addition, so it is an abelian group of order 6. Also, we have, $1(1, 1) = (1, 1)$.

   $$2(1, 1) = (1, 1)(1, 1) = (1 \oplus_2 1, 1 \oplus_3 1) = (0, 2)$$

   $$3(1, 1) = (1, 0), 4(1, 1) = (0, 1), 5(1, 1) = (1, 2), 6(1, 1) = (0, 0).$$

   Thus, $o(1, 1) = 6 = o(\mathbb{Z}_2 \oplus \mathbb{Z}_3)$. Hence, $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic.

   Since any cyclic group of order n is isomorphic to $\mathbb{Z}_n$, we have

   $$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6.$$

3. Consider $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. We have $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0, 0), (0, 1) (1, 0), (1, 1)\}$.

   We see that the group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$ as $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not cyclic whereas $\mathbb{Z}_4$ is cyclic.

   For if, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is cyclic, then it has a generator whose order should be same as $o(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = 4$. But no element of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ has order 4. Note that $2(1, 1) = (0, 0)$, i.e., order of $(1, 1)$ is less than or equal to 2. Hence no element can be generator of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

   Note: From above examples we notice that if G and H are groups and $o(G) = m$, $o(H) = n$, then $o(G \oplus H) = mn$.

PROBLEM 9.1 Construct the Cayley table of the group $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

SOLUTION We have $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$. The Cayley table of $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is given by combining elements as $(a, b) \cdot (c, d) = (a \oplus_2 c, b \oplus_3 d)$.

Table 9.1: Cayley Table of $\mathbb{Z}_2 \oplus \mathbb{Z}_3$

	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 0)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 1)	(0, 1)	(0, 2)	(0, 0)	(1, 1)	(1, 2)	(1, 0)
(0, 2)	(0, 2)	(0, 0)	(0, 1)	(1, 2)	(1, 0)	(1, 1)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 1)	(1, 1)	(1, 2)	(1, 0)	(0, 1)	(0, 2)	(0, 0)
(1, 2)	(1, 2)	(1, 0)	(1, 1)	(0, 2)	(0, 0)	(0, 1)

From the table it can be observed that $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is abelian.

9.2 Properties of External Direct Products

The next theorem provides us a simple way of determining the order of an element in an external direct product.

Theorem 9.2: Let $G_1, G_2, \ldots, G_n$ be n finite groups. Let $x = (x_1, x_2, \ldots, x_n) \in G_1 \oplus G_2 \oplus \ldots \oplus G_n$. Then, $o(x) = \text{lcm}(o(x_1), o(x_2), \ldots, o(x_n))$.

Proof: We first prove the result when the external direct product consists of only two factors.

Let $(a, b) \in G_1 \oplus G_2$. Let $o(a) = m$, $o(b) = n$ and let $k = \text{lcm}(m, n)$.

Then $(a, b)^k = (a^k, b^k) = (e_1, e_2)$ (since $o(a) = m$ and $m \mid k$)

Now suppose $(a, b)^t = (e_1, e_2)$. Then, $(a^t, b^t) = (e_1, e_2)$.

Thus, $a^t = e_1$ and $b^t = e_2$ and therefore, $m \mid t$ and $n \mid t$.

Hence $\text{lcm}(m, n) \mid t$. So, $o(a, b) = k = \text{lcm}(o(a), o(b))$.

Now let, $x = (x_1, x_2, \ldots, x_n) \in G_1 \oplus G_2 \oplus \ldots \oplus G_n$ and let $o(x_i) = m_i$ for all $i = 1, 2, \ldots, n$.

Let $k = \text{lcm}(m_1, m_2, \ldots, m_n)$. We will show that $o(x) = k$.

Since $o(x_i) = m_i$, therefore, $x_i^{m_i} = e_i$, for all $i = 1, 2, \ldots, n$.

Also $k = \text{lcm}(m_1, m_2, \ldots, m_n)$, there exist positive integers r_i, $i = 1, 2, \ldots, n$, such that $k = m_i r_i$.

Therefore, $x^k = (x_1, x_2, \ldots, x_n)^k = (x_1^k, x_2^k, \ldots, x_n^k)$

$$= (x_1^{m_1 r_1}, x_2^{m_2 r_2}, \ldots, x_n^{m_n r_n})$$

$$= (e_1, e_2, \ldots, e_n) \quad (\text{since } x_i^{m_i r_i} = (x_i^{m_i})^{r_i} = (e_i)^{r_i} = e_i)$$

Now, let $x^t = e$, then $(x_1, x_2, \ldots, x_n)^t = (e_1, e_2, \ldots, e_n)$.

As seen above we have $m_i \mid t$ for all i and so $k \mid t$.

Therefore, $o(x) = k = \text{lcm}(o(x_1), o(x_2), \ldots, o(x_n))$.

Problem 9.2 Find the number of elements of order 5 in $\mathbb{Z}_5 \oplus \mathbb{Z}_{15}$.

Solution Let $(a, b) \in \mathbb{Z}_5 \oplus \mathbb{Z}_{15}$. To find all those elements (a, b) whose order is 5.

Now $a \in \mathbb{Z}_5$ gives $o(a) = 1$ or 5. Similarly $b \in \mathbb{Z}_{15}$ implies $o(b) = 1, 3, 5$ or 15.

Now $o((a, b)) = 5$ means $\text{lcm}(o(a), o(b)) = 5$.

There are following possibilities:

(i) $o(a) = 5$, $o(b) = 1$.

The number of elements of order 5 in $\mathbb{Z}_5$ is $\varphi(5) = 4$. Also, the number of elements of order 1 in $\mathbb{Z}_{15}$ is $\varphi(1) = 1$. Thus the number of elements of order 5 in $\mathbb{Z}_5 \oplus \mathbb{Z}_{15}$ is $4.1 = 4$.

(ii) $o(a) = 1$, $o(b) = 5$.

The number of elements of order 1 in $\mathbb{Z}_5$ is $\varphi(1) = 1$. Also, the number of elements of order 5 in $\mathbb{Z}_{15}$ is $\varphi(5) = 4$. Thus the number of elements of order 5 in $\mathbb{Z}_5 \oplus \mathbb{Z}_{15}$ is $1.4 = 4$.

(iii) $o(a) = 5$, $o(b) = 5$.

The number of elements of order 5 in $\mathbb{Z}_5$ is $\varphi(5) = 4$. Also, the number of elements of order 5 in $\mathbb{Z}_{15}$ is $\varphi(5) = 4$. Thus the number of elements of order 5 in $\mathbb{Z}_5 \oplus \mathbb{Z}_{15}$ is $4.4 = 16$.

Therefore, the total number of elements of order 5 in $\mathbb{Z}_5 \oplus \mathbb{Z}_{15}$ is $4 + 4 + 16 = 24$.

PROBLEM 9.3 Find the order of the element $\alpha = (3, 3, (1\ 2\ 4)(5\ 7))$ in $U(8) \oplus \mathbb{Z}_{12} \oplus S_7$.

SOLUTION The element 3 in $U(8)$ has order 2 since $3^2 = 3.3 \bmod 8 \equiv 1$. Also in $\mathbb{Z}_{12}$, we have $(3 + 3 + 3 + 3) \bmod 12 \equiv 0$. So, $o(3) = 4$ in $\mathbb{Z}_{12}$.

In S_7, $o((1\ 2\ 4)(5\ 7)) = \text{lcm}\ (3, 2) = 6$.

Thus $o(\alpha) = \text{lcm}\ (2, 4, 6) = 12$.

THEOREM 9.3: Let G_1 and G_2 be finite cyclic groups. Then $G_1 \oplus G_2$ is cyclic if and only if $o(G_1)$ and $o(G_1)$ are relatively prime.

Proof: Let $o(G_1) = m_1$ and $o(G_2) = m_2$. Since G_1 and G_2 are cyclic, let

$G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2 \rangle$. Then, $o(g_1) = m_1$ and $o(g_2) = m_2$ and $o(G_1 \oplus G_2) = m_1 m_2$.

Suppose $o(G_1)$ and $o(G_2)$ are relatively prime, i.e., $\gcd(m_1, m_2) = 1$. We will prove that $G_1 \oplus G_2$ is cyclic.

Consider $(g_1, g_2)^{m_1 m_2} = ({g_1}^{m_1 m_2}, {g_2}^{m_1 m_2}) = (({g_1}^{m_1})^{m_2}, ({g_2}^{m_2})^{m_1}) = (e_1, e_2)$.

Suppose that $(g_1, g_2)^t = (e_1, e_2)$. Then $({g_1}^t, {g_2}^t) = (e_1, e_2)$.

Therefore, ${g_1}^t = e_1$ and ${g_2}^t = e_2$.

Hence $m_1 | t$ and $m_2 | t$ and as $\gcd(m_1, m_2) = 1$, we have $m_1 m_2 | t$.

Therefore, $o(g_1, g_2) = m_1 m_2$ and hence $G_1 \oplus G_2 = \langle (g_1, g_2) \rangle$.

Conversely, let $G_1 \oplus G_2$ be cyclic. Let $G_1 \oplus G_2 = \langle (a, b) \rangle$.

Let $k = \gcd(m_1, m_2)$. We need to show that $k = 1$.

Consider, $(a,b)^{m_1 m_2 / k} = (a^{m_1 m_2 / k}, b^{m_1 m_2 / k}) = ((a^{m_1})^{m_2 / k}, (b^{m_2})^{m_1 / k}) = (e_1, e_2)$.

Thus, $o(a, b) \Big| \dfrac{m_1 m_2}{k}$.

Also $o(G_1 \oplus G_2) = m_1m_2 = o(\langle(a, b)\rangle)$, therefore $m_1m_2 \mid \frac{m_1m_2}{k}$.

This gives $\frac{k(m_1\, m_2)}{k} \Big| \frac{m_1m_2}{k}$ and so $k \mid 1$.

Hence $k = 1$, i.e., $o(G_1)$ and $o(G_2)$ are relatively prime.

Problem 9.4 Prove that $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

Solution Since $\mathbb{Z}_n$ is a cyclic group, therefore by above theorem 9.3, we have $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$. Also, $o(\mathbb{Z}_m \oplus \mathbb{Z}_n) = mn$.

We also have that a cyclic group of order mn is isomorphic to $\mathbb{Z}_{mn}$. Thus, the result follows.

Remarks

- Let $G_1, G_2, \ldots, G_n$ be finite cyclic groups. Then the external direct product $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ is cyclic if and only if $o(G_i)$ and $o(G_j)$ are relatively prime for all $i \neq j$.
- $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_k} \cong \mathbb{Z}_{m_1m_1\ldots m_k}$ if and only if m_i and m_j are relatively prime for all $i \neq j$.

Problem 9.5 What is the order of any non- identity element in $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Solution We have $o(\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3) = 27$. So, the possible orders of the non-identity elements are 3, 9 or 27.

Since for any $(a, b, c) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $o((a, b, c)) = \text{lcm}(o(a), o(b), o(c))$ can never be 9 or 27. So $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ has no element of order 9 and 27.

Thus, the order of any non- identity element in $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ is 3.

Problem 9.6 Find all subgroups of order 3 in $\mathbb{Z}_9 \oplus \mathbb{Z}_3$.

Solution Since a group of prime order is cyclic, so every subgroup of order 3 is cyclic and these are those subgroups which are generated by the elements of order 3.

Let $(a, b) \in \mathbb{Z}_9 \oplus \mathbb{Z}_3$, then $o((a, b)) = 3$ if $\text{lcm}(o(a), o(b)) = 3$.

The only possibilities are:

(i) $o(a) = 1$, $o(b) = 3$.

The number of elements of order 1 in $\mathbb{Z}_9$ is $\varphi(1) = 1$. Also, the number of elements of order 3 in $\mathbb{Z}_3$ is $\varphi(3) = 2$. Thus the number of elements of order 3 in $\mathbb{Z}_9 \oplus \mathbb{Z}_3$ is $1.2 = 2$. Also here $a = 0$ and $b = 1$ or 2.

Therefore, $(a, b) = (0, 1), (0, 2)$.

(ii) $o(a) = 3$, $o(b) = 1$.

The number of elements of order 3 in $\mathbb{Z}_9$ is $\varphi(3) = 2$. Also, the number of elements of order 1 in $\mathbb{Z}_3$ is $\varphi(1) = 1$. Thus the number of elements of order 3 in $\mathbb{Z}_9 \oplus \mathbb{Z}_3$ is $2.1 = 2$. Also here $a = 3$ or 6 and $b = 0$.

Therefore, $(a, b) = (3, 0), (6, 0)$.

(iii) $o(a) = 3$, $o(b) = 3$.

The number of elements of order 3 in $\mathbb{Z}_9$ is $\varphi(3) = 2$. Also, the number of elements of order 3 in $\mathbb{Z}_3$ is $\varphi(3) = 2$. Thus the number of elements of order 3 in $\mathbb{Z}_9 \oplus \mathbb{Z}_3$ is $2.2 = 4$. Also here $a = 3$ or 6 and $b = 1$ or 2.

Therefore, $(a, b) = (3, 1), (3, 2), (6, 1), (6, 2)$.

Thus, the total number of elements of order 3 in $\mathbb{Z}_9 \oplus \mathbb{Z}_3$ is $2 + 2 + 4 = 8$.

Since an element and its inverse generates the same group and the pair of inverses are:

$$(0, 1), (0, 2); (3, 0), (6, 0); (3, 1), (6, 2); (3, 2), (6, 1)$$

Therefore, the four distinct cyclic subgroups of order 3 in $\mathbb{Z}_9 \oplus \mathbb{Z}_3$ are

$\langle(0, 1)\rangle, \langle(3, 0)\rangle, \langle(3, 1)\rangle, \langle(3, 2)\rangle$.

PROBLEM 9.7 Find all subgroups of order 4 in $\mathbb{Z}_4 \oplus \mathbb{Z}_2$.

SOLUTION

We have $\mathbb{Z}_4 \oplus \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)\}$

Now let $(a, b) \in \mathbb{Z}_4 \oplus \mathbb{Z}_2$, then $o((a, b)) = 4$ if lcm $(o(a), o(b)) = 4$.

There are following possibilities:

(i) $o(a) = 4$, $o(b) = 1$.

In this case the number of elements of order 4 in $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ is $\varphi(4)\varphi(1) = 2.1 = 2$. Also here $a = 1, 3$ and $b = 0$. Therefore, $(a, b) = (1, 0), (3, 0)$.

(ii) $o(a) = 4$, $o(b) = 2$.

In this case the number of elements of order 4 in $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ is $\varphi(4)\varphi(2) = 2.1 = 2$. Also here $a = 1, 3$ and $b = 1$. Therefore, $(a, b) = (1, 1), (3, 1)$.

Thus, there are four elements of order 4 in $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. Also we have

$(1, 0)^{-1} = (3, 0)$ and $(1, 1)^{-1} = (3, 1)$.

Thus, there are only two cyclic subgroups of order 4 in $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, namely, $\langle(1, 0)\rangle, \langle(1, 1)\rangle$.

Also, $\{(0, 0), (0, 1), (2, 0), (2, 1)\}$ is a non- cyclic subgroup of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$.

Problem 9.8 Let H and K be two groups. Prove that $H \oplus K$ is abelian if and only if H and K are abelian.

Solution Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$ be arbitrary elements.

Let $H \oplus K$ be abelian.

Then, $(h_1h_2, k_1k_2) = (h_1, k_1)\cdot(h_2, k_2) = (h_2, k_2)\cdot(h_1, k_1) = (h_2h_1, k_2k_1)$.

Thus, $h_1h_2 = h_2h_1$ and $k_1k_2 = k_2k_1$ and so, H and K are abelian.

Conversely, let H and K be abelian. To show $H \oplus K$ is abelian.

We have $(h_1, k_1)\cdot(h_2, k_2) = (h_1h_2, k_1k_2) = (h_2h_1, k_2k_1) = (h_2, k_2)\cdot(h_1, k_1)$.

Thus $H \oplus K$ is abelian.

Problem 9.9 Give an example of a non-abelian group of order 48.

Solution Consider the group $S_4 \oplus \mathbb{Z}_2$. Then $o(S_4 \oplus \mathbb{Z}_2) = (4!)\cdot 2 = 48$. Also since S_4 is non abelian, we have $S_4 \oplus \mathbb{Z}_2$ is non abelian.

Problem 9.10 Let H be a normal subgroup of a group G and K be a normal subgroup of a group G'. Prove that $H \oplus K$ is a normal subgroup of $G \oplus G'$.

Solution Let $(h_1, k_1), (h_2, k_2) \in H \oplus K$ be two elements. Then,

$$(h_1, k_1)(h_2, k_2)^{-1} = (h_1, k_1)(h_2^{-1}, k_2^{-1}) = (h_1h_2^{-1}, k_1k_2^{-1}) \in H \oplus K.$$

Thus, $H \oplus K$ is a subgroup of $G \oplus G'$.

Now, let $(g, g') \in G \oplus G'$ be arbitrary element. Let $(h, k) \in H \oplus K$. Then,

$$(g, g')^{-1}(h, k)(g, g') = (g^{-1}, g'^{-1})\,(hg, kg') = (g^{-1}hg, g'^{-1}kg') \in H \oplus K$$

(since $H \trianglelefteq G$ and $K \trianglelefteq G'$)

Thus, $H \oplus K$ is a normal subgroup of $G \oplus G'$.

Problem 9.11 Prove that $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Solution In $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, the element (1, 1) has order 8 (since lcm(8, 2) = 8)

However, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ has no element of order 8 as in this group the maximum order for an element can be 4 (since lcm(4, 4) = 4)

Therefore, $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

9.3 $U(n)$ as External Direct Products

Definition 9.3: Let k be a divisor of n. Define

$$U_k(n) = \{x \in U(n) : x \equiv 1 \bmod k\}$$

Thus $U_k(n)$ is the set of all those elements of $U(n)$ that leaves the remainder 1 when divided by k.

Example: We have $U(35) = \{x < 35 : \gcd(x, 35) = 1\}$

$= \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$

Also 5 and 7 are divisors of 35.

Thus, $U_5(35) = \{1, 6, 11, 16, 26, 31\}$ and $U_7(35) = \{1, 8, 22, 29\}$

Theorem 9.4: Let m and n be relatively prime, then $U(mn)$ is isomorphic to $U(m) \oplus U(n)$.

Proof: Define a map $f : U(mn) \to U(m) \oplus U(n)$ by

$$f(x) = (x \bmod m, x \bmod n)$$

To show that f is well defined, we need to show that if $x \in U(mn)$ then $x \bmod m \in U(m)$ and $x \bmod n \in U(n)$.

Now $x \in U(mn)$ gives $\gcd(x, mn) = 1$. This gives $\gcd(x, m) = 1$ and $\gcd(x, n) = 1$.

Let $x \bmod m = u$, then $x = mt + u$ for some $t \in \mathbb{Z}$.

Therefore $\gcd(x, m) = 1$

$\Leftrightarrow$ $ax + mb = 1$ for some $a, b \in \mathbb{Z}$.

$\Leftrightarrow$ $a(mt + u) + bm = 1$

$\Leftrightarrow$ $au + m(at + b) = 1$

$\Leftrightarrow$ $\gcd(u, m) = 1$

$\Leftrightarrow$ $\gcd(x \bmod m, m) = 1$

$\Leftrightarrow$ $x \bmod m \in U(m)$

Similarly, it can be shown that $\gcd(x, n) = 1 \Leftrightarrow x \bmod n \in U(n)$.

Thus, $(x \bmod m, x \bmod n) \in U(m) \oplus U(n)$ whenever $x \in U(mn)$ and so f is well defined.

Now let $x \in \ker f$, then $f(x) = (1, 1) \Rightarrow (x \bmod m, x \bmod n, 8) = (1, 1)$

$\Rightarrow$ $x \bmod m = 1, x \bmod n = 1$

$\Rightarrow$ $m \mid (x - 1), \quad n \mid (x - 1)$

$\Rightarrow$ $mn \mid (x - 1)$

$\Rightarrow$ $x \equiv 1 \bmod mn$

$\Rightarrow$ $x = 1$ (as $x \in U(mn)$ so $x < mn$)

Therefore $\ker f = \{1\}$ and hence f is one–one.

Let $(u, v) \in U(m) \oplus U(n)$ then since m and n are relatively prime, there exists integers a, b such that $am + bn = 1$.

Let $x = (amv + bnu) \bmod mn$, then $amv + bnu = x + mnt$ for some $t \in \mathbb{Z}$.

Then, $(amv + bnu) \bmod m = (x + mnt) \bmod m$

$\Rightarrow$ $bnu \bmod m = x \bmod m$

$\Rightarrow$ $x \bmod m = (bn \bmod m)(u \bmod m)$

$\Rightarrow$ $x \bmod m = (u \bmod m) = u$ as $u \in U(m)$.

Similarly, it can be shown that $x \bmod n = v$.

We now show that $x \in U(mn)$, i.e., $\gcd(x, mn) = 1$.

Now, $u \in U(m) \Rightarrow \gcd(u, m) = 1 \Rightarrow \gcd(x \bmod m, m) = 1 \Rightarrow \gcd(x, m) = 1$ and $v \in U(n) \Rightarrow \gcd(x, n) = 1$.

Since $\gcd(x, m) = 1$, there exist integers r, s such that $rx + sm = 1$. Also $\gcd(x, n) = 1$, so there exist integers t, k such that $tx + kn = 1$.

Therefore, $1 = (rx + sm)(tx + kn) = x(rtx + stm + knr) + mn(ks)$.

So, $\gcd(x, mn) = 1$.

Thus, there exists $x \in U(mn)$ such that $f(x) = (x \bmod m, x \bmod n) = (u, v)$.

Therefore f is onto.

Now $f(xy) = (xy \bmod m, xy \bmod n)$

$= ((x \bmod m)(y \bmod m), (x \bmod n)(y \bmod n))$

$= (x \bmod m, x \bmod n) \cdot (y \bmod m, y \bmod n)$

$= f(x) \cdot f(y)$

Thus f is a homomorphism and hence an isomorphism.

Corollary 9.1: Let m and n be relatively prime, then $U_m(mn) \cong U(n)$ and $U_n(mn) \cong U(m)$.

Proof: This can be proved by defining a map $\varphi : U_m(mn) \to U(n)$ by

$$\varphi(x) = x \bmod n.$$

Then as shown in the proof of theorem 9.4, it can be proved that φ is an isomorphism.

Similarly, defining $\theta : U_n(mn) \to U(m)$ by $\theta(x) = x \bmod m$, and showing that θ is a bijective homomorphism, we have the result.

Corollary 9.2: $U(m_1 m_2 \ldots m_k) \cong U(m_1) \oplus U(m_2) \oplus \ldots \oplus U(m_k)$ if and only if m_i and m_j are relatively prime for all $i \neq j$.

Proof: The result can be proved by applying induction on k.

Example: Consider the group $U(105)$. We have $105 = 5.21 = 7.15 = 3.5.7$.

Thus $U(105) \cong U(5) \oplus U(21)$. Also $U(105) \cong U(7) \oplus U(15)$ and

$$U(105) \cong U(3) \oplus U(5) \oplus U(7)$$

Further, $U_7(105) \cong U(15)$, $U_{15}(105) \cong U(7)$, $U_5(105) \cong U(21)$, $U_{21}(105) \cong U(5)$, $U_{35}(105) \cong U(3)$.

THEOREM 9.5:

1. $U(2) \cong \{0\}$.
2. $U(4) \cong \mathbb{Z}_2$
3. $U(2^n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$, $n \geq 3$.
4. $U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}}$, p is odd prime.

Proof: The proof is out of the scope of this book.

PROBLEM 9.12 Express $U(165)$ and $U(720)$ as an external direct product of cyclic additive groups of the form $\mathbb{Z}_n$.

SOLUTION We have

$$U(165) = U(3.5.11) \cong U(3) \oplus U(5) \oplus U(11)$$
$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10}$$

Similarly, $U(720) = U(5.9.16) \cong U(5) \oplus U(9) \oplus U(16)$
$$\cong U(5) \oplus U(3^2) \oplus U(2^4)$$
$$\cong \mathbb{Z}_4 \oplus \mathbb{Z}_{3^2-3^1} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^4-2}$$
$$\cong \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$$

PROBLEM 9.13 Express $U(165)$ as an external direct product of U groups in different ways.

SOLUTION We have $U(165) = U(3.5.11) \cong U(3) \oplus U(5) \oplus U(11)$
$$\cong U(15) \oplus U(11)$$
$$\cong U(5) \oplus U(33)$$
$$\cong U(3) \oplus U(55)$$

PROBLEM 9.14 Prove that $U(54)$ is a cyclic group.

SOLUTION We have $U(54) = U(2.3^3) \cong U(2) \oplus U(3^3) \cong U(2) \oplus \mathbb{Z}_{3^3-3^2}$
$$\cong U(2) \oplus \mathbb{Z}_{18}$$

Now since $U(2)$ and $\mathbb{Z}_{18}$ are cyclic groups and $(o(U(2)), o(\mathbb{Z}_{18})) = \gcd(1, 18) = 1$, we have that $U(2) \oplus \mathbb{Z}_{18}$ is cyclic and hence $U(54)$ is cyclic.

PROBLEM 9.15 Find the number of elements of order 4 and order 2 in $\text{Aut}(\mathbb{Z}_{20})$.

SOLUTION We know $\text{Aut}(\mathbb{Z}_n) \cong U(n)$.

Thus, $\text{Aut}(\mathbb{Z}_{20}) \cong U(20) \cong U(2^2 \cdot 5) \cong U(2^2) \oplus U(5) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$

We have already seen in problem 9.7 that $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ has four elements of order 4.

Now let $(a, b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_4$, then $o((a, b)) = 2$ if lcm $(o(a), o(b)) = 2$.

There are following possibilities:

(i) $o(a) = 2$, $o(b) = 1$.
In this case the number of elements of order 2 in $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ is $\varphi(2)\varphi(1) = 1.1 = 1$.

(ii) $o(a) = 1$, $o(b) = 2$.
In this case the number of elements of order 2 in $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ is $\varphi(1)\ \varphi(2) = 1.1 = 1$.

(iii) $o(a) = 2$, $o(b) = 2$.
In this case the number of elements of order 2 in $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ is $\varphi(2)\ \varphi(2) = 1.1 = 1$.
Thus, there are 3 elements of order 2 in $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.

Problem 9.16 What is the largest possible order for an element in the group $U(900)$.

Solution We have

$$U(900) = U(4.9.25) \cong U(4) \oplus U(9) \oplus U(25) \cong U(2^2) \oplus U(3^2) \oplus U(5^2)$$
$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{20}$$

Now, let $(a, b, c) \in \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{20}$ Then, $a \in \mathbb{Z}_2$ gives $o(a) = 1$ or 2.

Similarly, $b \in \mathbb{Z}_6$ implies $o(b) = 1$, 2, 3 or 6. Also $c \in \mathbb{Z}_{20}$ gives $o(c) = 1$, 2, 4, 5, 10 or 20.

Thus, the largest possible order of $(a, b, c) = \text{lcm}(2, 6, 20) = 60$.

Problem 9.17 Let G be a group of order 4 with the property that $x^2 = e$ for all x in G. Prove that $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Solution Since $o(G) = 4$ and $x^2 = e$ for all x in G, therefore G has exactly three elements of order 2.

Also $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Since $\mathbb{Z}_4$ being cyclic has exactly $\varphi(2) = 1$ element of order 2. So $G \ncong \mathbb{Z}_4$.

Thus, $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Problem 9.18 Show that there exists no onto homomorphism from $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Solution Suppose $f : \mathbb{Z}_8 \oplus \mathbb{Z}_2 \to \mathbb{Z}_4 \oplus \mathbb{Z}_4$ is an onto homomorphism. Then

$$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \cong \frac{\mathbb{Z}_8 \oplus \mathbb{Z}_2}{\ker f}$$

$$\Rightarrow \qquad o(\mathbb{Z}_4 \oplus \mathbb{Z}_4) = o\left(\frac{\mathbb{Z}_8 \oplus \mathbb{Z}_2}{\ker f}\right) = \frac{o(\mathbb{Z}_8 \oplus \mathbb{Z}_2)}{o(\ker f)}$$

$$\Rightarrow \qquad 16 = \frac{16}{o(\ker f)}$$

Thus $o(\ker f) = 1$ and so f is one-one.

Therefore, f is an isomorphism, i.e., $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Now, $o((1, 0)) = 8$ in $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, but there is no element in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, whose order is 8.

Therefore, we get a contradiction.

Hence there does not exist any onto homomorphism from $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Problem 9.19 Show that there exists no onto homomorphism from $\mathbb{Z}_{16} \oplus \mathbb{Z}_2$ to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Solution Suppose $f : \mathbb{Z}_{16} \oplus \mathbb{Z}_2 \to \mathbb{Z}_4 \oplus \mathbb{Z}_4$ is an onto homomorphism. Then,

$$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \cong \frac{\mathbb{Z}_{16} \oplus \mathbb{Z}_2}{\ker f}$$

$$\Rightarrow o(\mathbb{Z}_4 \oplus \mathbb{Z}_4) = \frac{o(\mathbb{Z}_{16} \oplus \mathbb{Z}_2)}{o(\ker f)} \Rightarrow 16 = \frac{32}{o(\ker f)} \Rightarrow o(\ker f) = 2$$

$\Rightarrow \ker f = \{(0, 0), (8, 1)\}$ or $\{(0, 0), (8, 0)\}$ or $\{(0, 0), (0, 1)\}$

Suppose $\ker f = \{(0, 0), (8, 0)\} = k$ (say)

Let $(1, 0) + k \in \dfrac{\mathbb{Z}_{16} \oplus \mathbb{Z}_2}{\ker f}$.

Then $\underbrace{((1, 0) + k) + ((1, 0) + k) + \ldots + ((1, 0) + k)}_{(8 \text{ times})} = (8, 0) + k = k.$

So, $o((1, 0) + k) = 8$.

But $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ has no element of order 8, which is a contradiction, therefore homomorphism is not onto.

Suppose $k = \{(0, 0), (8, 1)\}$ or $k = \{(0, 0), (0, 1)\}$

Consider $(1, 1) + k \in \dfrac{Z_{16} \oplus Z_2}{k}$.

Then $\underbrace{((1, 1) + k) + ((1, 1) + k) + \ldots + ((1, 1) + k)}_{(16 \text{ times})} = (0, 0) + k = k$

Thus, $o((1, 1) + k) = 16$. But $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ does not have an element of order 16.

Therefore, this can't be onto homomorphism.

Problem 9.20 Show that $U(30)/U_5(30)$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_4$.

Solution We have $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$. So $U_5(30) = \{1, 11\}$.

Now, $o(U(30)/U_5(30)) = \dfrac{o(U(30))}{o(U_5(30))} = \dfrac{8}{2} = 4$. Let $K = U_5(30)$.

Then $U(30)/K = \{xK : x \in U(30)\} = \{K, 7K, 13K, 19K\}$

where $7K = \{7, 17\}$, $13K = \{13, 23\}$, $19K = \{19, 29\}$.

Also $U(30)/K = \langle 7K \rangle$. So, it is a cyclic group of order 4 and hence is isomorphic to $\mathbb{Z}_4$.

In external direct product, we combined two or more unrelated groups to form a new group with new binary operations. However, in internal direct product we use the normal subgroups of the group G and the operations of G to form new group.

9.4 Internal Direct Products

Definition 9.4: Let $K_1, K_2, \ldots, K_n$ be a finite collection of normal subgroups of a group G. Then G is the **internal direct product** of $K_1, K_2, \ldots, K_n$, written as $G = K_1 \times K_2 \times \ldots \times K_n$, if

(i) $G = K_1 K_2 \ldots K_n = \{k_1 k_2 \ldots k_n : k_i \in K_i\}$

(ii) $(K_1 K_2 \ldots K_i) \cap K_{i+1} = \{e\}$ for $i = 1, 2, \ldots n-1$.

Definition 9.5: Let K_1 and K_2 be normal subgroups of a group G. Then G is the **internal direct product** of K_1 and K_2 written as $G = K_1 \times K_2$, if

(i) $G = K_1 K_2 = \{k_1 k_2 : k_i \in K_i\}$

(ii) $K_1 \cap K_2 = \{e\}$.

Example: Let G be a cyclic group of order 6 and let $G = \langle a \rangle = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$.

Let $K_1 = \{e, a^2, a^4\}$ and $K_2 = \{e, a^3\}$. Then G being cyclic is abelian, so K_1 and K_2 are normal subgroups of G. Also, $K_1 \cap K_2 = \{e\}$.

Further, $K_1 K_2 = \{e, a^3, a^2, a^5, a^4, a\} = G$. Thus, we have $G = K_1 \times K_2$.

Theorem 9.6: Let $K_1, K_2, \ldots, K_n$ be a finite collection of normal subgroups of a group G. Then G is the internal direct product of $K_1, K_2, \ldots, K_n$ if and only if

(i) $G = K_1 K_2 \ldots K_n$

(ii) Any $g \in G$ can be uniquely expressed as $g = k_1 k_2 \ldots k_n$, $k_i \in K_i$.

Proof: Suppose (i) and (ii) holds. To show that G is an internal direct product of $K_1, K_2, \ldots, K_n$, we need to show that $(K_1 K_2 \ldots K_i) \cap K_{i+1} = \{e\}$.

Let $x \in (K_1 K_2 \ldots K_i) \cap K_{i+1}$, then $x = k_1 k_2 \ldots k_i$, $k_i \in K_i$ and $x = k_{i+1}$, $k_{i+1} \in K_{i+1}$.

Thus, $x = k_1 k_2 \ldots k_i e e \ldots e$ and $x = e e \ldots e k_{i+1} e \ldots e$. Since the expression of x as product of elements of $K_1 K_2 \ldots K_n$ is unique, we have $k_1 = k_2 = \ldots = k_i = k_{i+1} = e$ and so $x = e$.

Therefore $(K_1 K_2 \ldots K_i) \cap K_{i+1} = \{e\}$ and hence G is an internal direct product of $K_1, K_2, \ldots, K_n$.

Conversely, let G be an internal direct product of $K_1, K_2, \ldots, K_n$, then by definition $G = K_1 K_2 \ldots K_n$.

Now let $g \in G$ be such that $g = k_1 k_2 \ldots k_n$ and $g = h_1 h_2 \ldots h_n$, $k_i, h_i \in K_i$.

We first show that $K_i \cap K_j = \{e\}$ for all $i \neq j$. Let $x \in K_i \cap K_j$, then $x \in K_i$ and $x \in K_j$.

Now $x \in K_j$ implies $x \in K_1K_2 \ldots K_{i-1}K_{i+1} \ldots K_j \ldots K_n$.

Thus $x \in (K_1K_2 \ldots K_{i-1}K_{i+1} \ldots K_j \ldots K_n) \cap K_i = \{e\}$ and so $x = e$.

Therefore, $K_i \cap K_j = \{e\}$ for all $i \neq j$. Hence $k_ik_j = k_jk_i$ for all $k_i \in K_i$, $k_j \in K_j$.

Now, $k_1k_2 \ldots k_n = h_1h_2 \ldots h_n$ gives $k_2 \ldots k_n = k_1^{-1} h_1h_2 \ldots h_n$.

This implies $k_3 \ldots k_n = (k_1^{-1}h_1)(k_2^{-1}h_2) \ldots h_n$.

Continuing in this way we get, $k_nh_n^{-1} = (k_1^{-1}h_1)(k_2^{-1}h_2) \ldots (k_{n-1}^{-1}h_{n-1})$.

Thus $k_nh_n^{-1} \in K_1K_2 \ldots K_{n-1} \cap K_n = \{e\}$ and so $k_nh_n^{-1} = e$.

Therefore, $k_n = h_n$. Similarly, $k_i = h_i$ for all i.

Thus, the representation is unique.

Theorem 9.7: Let $K_1, K_2, \ldots, K_n$ be a finite collection of normal subgroups of a group G. If G is the internal direct product of $K_1, K_2, \ldots, K_n$ then G is isomorphic to the external direct product of $K_1, K_2, \ldots, K_n$.

Proof: Let G be an internal direct product of $K_1, K_2, \ldots, K_n$. We need to show that $K_1 \times K_2 \times \ldots \times K_n \cong K_1 \oplus K_2 \oplus \ldots \oplus K_n$.

Define a map $f: K_1 \oplus K_2 \oplus \ldots \oplus K_n \to G$ by $f((k_1, k_2, \ldots, k_n)) = k_1k_2 \ldots k_n$, $k_i \in K_i$.

Now $(k_1, k_2, \ldots, k_n) = (k_1', k_2', \ldots, k_n')$

$\Rightarrow \quad k_i = k_i'$ for all i.

$\Rightarrow \quad k_1k_2 \ldots k_n = k_1'\, k_2' \ldots k_n'$

$\Rightarrow \quad f((k_1, k_2, \ldots, k_n)) = f((k_1', k_2', \ldots, k_n'))$

Thus f is well defined.

Also, $f((k_1, k_2, \ldots, k_n)) = f((k_1', k_2', \ldots, k_n'))$

$\Rightarrow \quad k_1k_2 \ldots k_n = k_1'\, k_2' \ldots k_n'$

$\Rightarrow \quad k_i = k_i'$ for all i (by previous theorem)

$\Rightarrow \quad (k_1, k_2, \ldots, k_n) = (k_1', k_2', \ldots, k_n')$

So, f is one–one.

For any $k_1k_2 \ldots k_n \in G$ there exists $(k_1, k_2, \ldots, k_n) \in K_1 \oplus K_2 \oplus \ldots \oplus K_n$ such that $f((k_1, k_2, \ldots, k_n)) = (k_1k_2 \ldots k_n)$. Thus, f is onto.

Now,

$$f((k_1, k_2, \ldots, k_n)\cdot(k_1', k_2', \ldots, k_n')) = f((k_1k_1', k_2k_2', \ldots, k_nk_n'))$$
$$= k_1k_1'k_2k_2' \ldots k_nk_n'$$
$$= (k_1k_2 \ldots k_n)\,(k_1'k_2' \ldots k_n')$$
$$= f((k_1, k_2, \ldots, k_n))\cdot f((k_1', k_2', \ldots, k_n'))$$

(since $K_i \cap K_j = \{e\}$ for all $i \neq j$ and so $k_ik_j = k_jk_i$).

Thus, f is a homomorphism and hence an isomorphism.

Problem 9.21 Show that D_4 cannot be expressed as an internal direct product of two proper subgroups.

Solution Let $D_4 = H \times K$, where $H, K \neq \{e\}$ or D_4. Then $D_4 = HK$ and $H \cap K = \{e\}$

Now since D_4 contains 8 elements, so $8 = o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = \dfrac{o(H)o(K)}{1}$.

Thus, $o(H)o(K) = 8$. We have two possibilities:

(i) $o(H) = 4$, $o(K) = 2$. Here $H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_4$ and $K \cong \mathbb{Z}_2$.

(ii) $o(H) = 2$, $o(K) = 4$. Here $H \cong \mathbb{Z}_2$ and $K \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_4$.

In both the cases H and K are abelian and so $H \oplus K$ is abelian.

Since $D_4 = H \times K \cong H \oplus K$, we have D_4 is abelian, which is not true.

Thus, D_4 cannot be expressed as an internal direct product of two proper subgroups.

Problem 9.22 Show that Q_8 cannot be expressed as an internal direct product of its non-trivial subgroups.

Solution We already know that all the subgroups of Q_8 are normal. Suppose that $Q_8 = H \times K$, where $H, K \neq \{e\}$ or Q_8. Then $Q_8 = HK$ and $H \cap K = \{e\}$.

But every subgroup of Q_8 contains both 1 and -1 and so the condition that $H \cap K = \{e\}$ is not satisfied.

Thus, we cannot express Q_8 as an internal direct product of its non-trivial subgroups.

Problem 9.23 Let $G = \mathbb{Z}$. Suppose $H = \langle 5 \rangle$ and $K = \langle 7 \rangle$. Show that $G = HK$. Is $G = H \times K$?

Solution The group of integers being an additive group, we have

$$HK = \{h + k : h \in H, k \in K\}$$

Since gcd(5, 7) = 1, there exist integers m and n such that $5m + 7n = 1$.

Now let $x \in G$, then $x = 1$. $x = 5mx + 7nx \in HK$. Thus, $G = HK$.

Also $H \cap K = \langle \text{lcm}(5, 7) \rangle = \langle 35 \rangle \neq \{1\}$. Thus, $G \neq H \times K$.

Problem 9.24 Show that a group of order 4 is either cyclic or is an internal direct product of two cyclic groups of order 2 each.

Solution Let G be a group of order 4. Let $a \in G$ be any element. Then $o(a) = 1$, 2 or 4.

If $o(a) = 4 = o(G)$, then G is cyclic group generated by a.

Now if $o(a) \neq 4$ and $a \neq e$, then $o(a) = 2$.

Let $x, y \in G$ be such that $o(x) = o(y) = 2$. Let $H = \langle x \rangle$ and $K = \langle y \rangle$.

Since G is abelian, H and K are normal subgroups of G and $H \cap K = \{e\}$.

Also, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = \dfrac{2.2}{1} = 4 = o(G)$. Thus, $G = HK$.

Therefore $G = H \times K$.

Problem 9.25 Show that $\mathbb{R}^* = \mathbb{R}^+ \times \{1, -1\}$, where $\mathbb{R}^*$ is the group of all non-zero real numbers under multiplication and $\mathbb{R}^+$ is the group of all positive real numbers under multiplication.

Solution To show that $\mathbb{R}^* = \mathbb{R}^+ \times \{1, -1\}$, we need to prove that

(i) $\mathbb{R}^+$ and $\{1, -1\}$ are normal subgroups of $\mathbb{R}^*$.

(ii) $\mathbb{R}^+ \cap \{1, -1\} = \{1\}$.

(iii) $\mathbb{R}^+ \{1, -1\} = \mathbb{R}^*$.

Since $\mathbb{R}^*$ is abelian, all subgroups of $\mathbb{R}^*$ are normal and so $\mathbb{R}^+$ and $\{1, -1\}$ are normal subgroups of $\mathbb{R}^*$.

Also $\mathbb{R}^+ \cap \{1, -1\} = \{1\}$.

We also have $\mathbb{R}^+\{1, -1\} \subseteq \mathbb{R}^*$ always. Otherway, let $x \in \mathbb{R}^*$ be any element. Then x can be positive or negative real number.

If x is positive then $x = x \cdot 1 \in \mathbb{R}^+\{1, -1\}$ and if x is negative then $(-x)$ is positive and $x = (-x)\cdot(-1) \in \mathbb{R}^+\{1, -1\}$.

Thus $\mathbb{R}^* \subseteq \mathbb{R}^+\{1, -1\}$ and so, $\mathbb{R}^+\{1, -1\} = \mathbb{R}^*$.

Therefore, $\mathbb{R}^* = \mathbb{R}^+ \times \{1, -1\}$.

9.5 Fundamental Theorem of Finite Abelian Groups

The Fundamental theorem of finite abelian groups is very important in the sense that it provides a way to construct all possible abelian groups of a particular order.

Definition 9.6: Let n be a positive integer. A sequence of positive integers $n_1, n_2, \ldots, n_k$ with $n_1 \geq n_2 \geq \ldots \geq n_k$ whose sum is n is called a **partition of n**. The number of partitions of n is denoted by $P(n)$.

Example: Let $n = 4$. Then $4 = 4$, $4 = 3 + 1$, $4 = 2 + 2$, $4 = 2 + 1 + 1$, $4 = 1 + 1 + 1 + 1$. Thus there are five different partitions of 4 and so $P(4) = 5$.

Similarly, one can see that there are three partitions namely, 3, $2 + 1$, $1 + 1 + 1$ of the integer 3. So $P(3) = 3$.

Problem 9.26 Let G be a finite abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where $H = \{x \in G : x^{p^n} = e\}$ and $K = \{x \in G : x^m = e\}$. Moreover, $o(H) = p^n$.

Proof: We first show that H and K are subgroups of G.

Since $e^{p^n} = e$, so $e \in H$ and therefore H is non empty. Now let $x, y \in H$.

Then $(xy^{-1})^{p^n} = x^{p^n} y^{-p^n} = e \cdot e = e$ (since G is abelian)

Thus, $xy^{-1} \in H$ and so H is a subgroup of G.

Similarly, it can be proved that K is a subgroup of G.

Also, since G is abelian, H and K are normal subgroups of G.

To show $G = H \times K$.

Since $p \nmid m$, we have $\gcd(p^n, m) = 1$. Thus, there exist integers r and s such that $rp^n + sm = 1$.

Now, let $x \in G$ be any element. Then,

$$x = x^1 = x^{rp^n + sm} = x^{rp^n} x^{sm} \in HK$$

(since, $(x^{sm})^{p^n} = (x^{p^n m})^s = e^s = e$, so $x^{sm} \in H$ and similarly $x^{rp^n} \in K$)

Thus, $G \subseteq HK$. Hence $G = HK$.

Now, let $y \in H \cap K$ be any element then $y \in H$ and $y \in K$.

Therefore, $y^{p^n} = e$ and $y^m = e$. So $o(y) \mid p^n$ and $o(y) \mid m$.

Since $\gcd(p^n, m) = 1$, $o(y) = 1$ and so, $y = e$.

Therefore $H \cap K = \{e\}$ and hence $G = H \times K$.

Now, $p^n m = o(G) = o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = \dfrac{o(H)o(K)}{1}$.

Thus, $o(H)o(K) = p^n m$.

Suppose $p|o(K)$, then by Cauchy's theorem there exists some $k \in K$ such that $o(k) = p$.

Now $k \in K$ implies $k^m = e$ and so $p|m$, which is not true

Thus, $p \nmid o(K)$, and so $o(K)$ is not a multiple of p. Hence $o(H) = p^n$.

THEOREM 9.8: Let G be an abelian group of prime power order and let a be an element of maximal order in G. Then G can be written as $\langle a \rangle \times K$, where K is a subgroup of G.

Proof:

Let $o(G) = p^n$. We will use induction on n to prove the result.

Let $n = 1$, then $o(G) = p$. This implies G is a cyclic group and let $G = \langle a \rangle$.

Then $o(a) = o(G) = p$.

Thus, a is an element of maximal order in G and $G = \langle a \rangle \times \{e\}$. Thus, result holds for $n = 1$.

Assume that the result holds for all abelian groups with order p^k, where $k < n$.

Let $a \in G$ be an element of maximal order, say $o(a) = p^m$. Let $H = \langle a \rangle$.

If $G = \langle a \rangle$ then we are done.

Let $G \neq \langle a \rangle = H$. Then there exists some element in G that does not belong to H.

Among all these elements of G choose an element b of smallest order such that $b \notin H$.

Now, $o(b^p) = \dfrac{o(b)}{\gcd(o(b), p)} = \dfrac{o(b)}{p} < o(b)$, so $b^p \in H = \langle a \rangle$.

Thus, $b^p = a^j$ for some j.

Since $o(a) = p^m$, which is maximal, so $x^{p^m} = e$ for all $x \in G$.

Therefore, $b^{p^m} = e$ as $b \in G$.

$\Rightarrow \quad (b^p)^{p^{m-1}} = e$

$\Rightarrow \quad (a^j)^{p^{m-1}} = e$ and so $o(a^j) \leq p^{m-1}$.

Thus, a^j is not a generator of H.

Also $H = \langle a \rangle$, so $o(H) = o(a) = p^m$ and hence $\gcd(p^m, j) \neq 1$.

This gives that p^m and j have a common factor and so $p \mid j$.

Therefore, $b^p = a^j = a^{pt}$ for some t.

Let $c = a^{-t}b$, then, if $c \in H$ we have $a^{-t}b \in H = \langle a \rangle$.

This gives $a^{-t}b = a_1$ for some $a_1 \in H$.

Then, $b = a^t a_1 \in H$, which is a contradiction. So $c \notin H$.

Since $c^p = a^{-pt}b^p = a^{-j}b^p = b^{-p}b^p = e$, thus $o(c) = p$.

Therefore, we have found an element $c \in G$ such that $c \notin H$ with $o(c) = p$.

But we have chosen b to have smallest order such that $b \notin H$. So $o(b) = p$.

Let $M = \langle b \rangle$, then $H \cap M$ is a subgroup of M and so $o(H \cap M) | o(M) = p$.

Thus, $o(H \cap M) = 1$ or p.

If $o(H \cap M) = p$ then $H \cap M = M$. Therefore, $b \in M$ means $b \in H \cap M$ and so $b \in H$ which is not true.

So, $o(H \cap M) = 1$ and thus, $H \cap M = \{e\}$.

Consider the group $G' = G/M$. Since $a \in G$ so, $Ma \in G/M = G'$.

Let us denote Ma by a'.

Then, $(a')^{o(a)} = (Ma)^{o(a)} = Ma^{o(a)} = M$ = identity of G'.

Thus, $o(a') | o(a)$ and so $o(a') \leq o(a)$.

Also $Ma^{o(a')} = (Ma)^{o(a')} = (a')^{o(a')}$ = identity of $G' = M$.

So $a^{o(a')} \in M$ and hence $a^{o(a')} \in H \cap M = \{e\}$.

Therefore, $a^{o(a')} = e$ and so $o(a) | o(a')$. Thus, $o(a) \leq o(a')$.

Then, $o(a) = o(a')$ and so a' is an element of maximal order in G'.

Also, $o(G') < o(G)$, so by induction, we have $G' = \langle a' \rangle \times T'$, where $T' \leq G'$.

Thus, $G' = \langle a' \rangle T'$, and $\langle a' \rangle \cap T' = \{M\}$.

Now $T' \leq G' = G/M$, so $T' = K/M$ where $K \leq G$.

To show $G = \langle a \rangle \times K$.

Let $x \in \langle a \rangle \cap K$, then $x \in \langle a \rangle$ and $x \in K$.

Then $x = a^i$ for some i and $x \in K$. Thus, $a^i \in K$ and so $Ma^i \in K/M$.

Thus, $(a')^i \in T'$. Also, $(a')^i \in \langle a' \rangle$. So, $(a')^i \in \langle a' \rangle \cap T' = \{M\}$.

Therefore, $(Ma)^i = M$ and so $Ma^i = M$. Thus, $a^i \in M$.

So, $a^i \in H \cap M = \{e\}$. Thus, $a^i = e$ and so $x = e$.

Therefore, $\langle a \rangle \cap K = \{e\}$.

Now let $x \in G$ then, $Mx \in G/M = \langle a' \rangle T'$.

Thus, $Mx = (a')^s y'$, where $y' \in T' = K/M$, so $y' = My$ for some $y \in K$.

Therefore, $Mx = (Ma)^s My = Ma^s My = Ma^s y$.

So, $xa^{-s}y^{-1} \in M \subseteq K$. This gives $xa^{-s}y^{-1} = k$, for some $k \in K$.

Then, $x = a^s yk = a^s z \in \langle a \rangle K$, where $z = yk \in K$.

So, $G = \langle a \rangle K$ and thus $G = \langle a \rangle \times K$, where $K \leq G$.

THEOREM 9.9: A finite abelian group of prime power order is an internal direct product of cyclic groups.

Proof: By Theorem 9.8, we can write $G = \langle a \rangle \times K$. Since, K is again a group of prime power order, we can write $K = \langle a_1 \rangle \times K_1$.

Proceeding in this way we can write

$$G = \langle a \rangle \times \langle a_1 \rangle \times ... \times \langle a_k \rangle$$

THEOREM 9.10: Let G be an abelian group of prime order p. Then, $G^p = \{x^p : x \in G\}$ is a subgroup of G.

Proof: Since $e \in G$, so $e^p \in G^p$. Thus $e \in G^p$ and therefore G^p is non empty.

Now let $x^p, y^p \in G^p$, then $x, y \in G$.

Then, $x^p y^{-p} = (xy^{-1})^p \in G^p$, as $xy^{-1} \in G$.

Therefore, G^p is a subgroup of G.

THEOREM 9.11: Let G be a finite abelian group such that $G = H \times K$ then, $G^p = H^p \times K^p$.

Proof: To show $G^p = H^p \times K^p$.

Let $x \in H^p \cap K^p$, then $x \in H^p$ and $x \in K^p$.

Therefore, $x = h^p$ and $x = k^p$ for some $h \in H$, $k \in K$.

This gives that $x \in H$ and $x \in K$ and so $x \in H \cap K = \{e\}$.

Therefore, $x = e$ and thus $H^p \cap K^p = \{e\}$.

Now let $x^p \in G^p$ be any element then $x \in G = HK$.

This implies $x = hk$ for some $h \in H$, $k \in K$.

Since G is abelian, $x^p = h^p k^p \in H^p K^p$.

Thus, $G^p \subseteq H^p K^p$ and so $G^p = H^p K^p$.

Therefore, $G^p = H^p \times K^p$.

THEOREM 9.12: Suppose that G is a finite abelian group of prime power order. If $G = H_1 \times H_2 \times ... \times H_m$ and $G = K_1 \times K_2 \times ... \times K_n$, where $H_i's$, $K_i's$ are non-trivial cyclic subgroups with $o(H_1) \geq o(H_2) \geq ... \geq o(H_m)$ and $o(K_1) \geq o(K_2) \geq ... \geq o(K_n)$, then $m = n$ and $o(H_i) = o(K_i)$ for all i.

Proof: Let $o(G) = p^k$. We use induction to prove the result.

If $k = 1$, then $o(G) = p$ and so G is cyclic and hence the result.

Let the result be true for all groups of order p^r, with $r < k$.

Since $G = H_1 \times H_2 \times ... \times H_m = K_1 \times K_2 \times ... \times K_n$, we have $G^p = H_1^p \times H_2^p \times ... \times H_{m'}^p = K_1^p \times K_2^p \times ... \times K_{n'}^p$ where m' is the largest integer i such that $o(H_i) > p$ and n' is the largest integer j such that $o(K_j) > p$.

Since, $o(G^p) < o(G)$, so by induction $m' = n'$ and $o(H_i^p) = o(K_i^p)$ for all $i = 1, 2, ... m'$.

Now, H_i is cyclic, so let $H_i = \langle a_i \rangle$ for all i. Then, ${H_i}^p = \langle {a_i}^p \rangle$ for all i.

Thus, $o({H_i}^p) = o({a_i}^p) = \dfrac{o(a_i)}{\gcd(o(a_i), p)} = \dfrac{o(H_i)}{p}$.

Now, $G = H_1 \times H_2 \times ... \times H_m$

$$\Rightarrow \quad o(G) = o(H_1)o(H_2) \ ... \ o(H_m) = p \cdot o({H_1}^p) \cdot p \cdot o({H_2}^p) \ ... p \cdot o({H_m}^p)$$

$$= p^m . o({H_1}^p) . \ o({H_2}^p) \ldots o({H_m}^p)$$

$$= p^m . o({H_1}^p) . \ o({H_2}^p) \ldots o({H_{m'}}^p)$$

$$= p^{m-m'} . o(H_1)o(H_2) \ldots o(H_{m'}) \text{ since } o({H_i}^p) = \frac{o(H_i)}{p} \text{ for all } i.$$

Similarly, $o(G) = p^{n-n'} . o(K_1)o(K_2) \ldots o(K_{n'})$.

Since by induction, $o(H_1)o(H_2) \ ... \ o(H_{m'}) = o(K_1)o(K_2) \ ... \ o(K_{n'})$, we have $p^{m-m'} = p^{n-n'}$ and so, $m - m' = n - n'$.

Therefore, as $m' = n'$ we have $m = n$. Also, $o(H_i) = o(K_i)$ for all $i = 1, 2, ... , m'$.

Thus, $o(H_i) = o(K_i)$ for all $i = 1, 2, ... , m$.

Theorem 9.13: Every finite abelian group is a direct product of cyclic groups of prime power order. Further, the factorization is unique except for the rearrangement of the factors.

Proof: Let G be a finite abelian group such that $o(G) = {p_1}^{m_1} {p_2}^{m_2} \ ... \ {p_k}^{m_k}$, where $p_i's$ are distinct primes. Letting $m = {p_2}^{m_2} ... \ {p_k}^{m_k}$ and using problem 9.26, we have $G = G_1 \times K$, where $G_1 = \{x \in G : x^{{p_1}^{m_1}} = e\}$ and $o(G_1) = {p_1}^{m_1}$.

Applying the same process to K as we did to G we get $K = G_2 \times K'$, with $o(G_2) = {p_2}^{m_2}$.

Continuing like this we get $G = G_1 \times G_1 \times ... \times G_k$ with $o(G_i) = {p_i}^{m_i}$.

Now, from Theorem 9.9, each G_i being a finite abelian group can be written as internal direct product of cyclic groups.

Also, from Theorem 9.12, it follows that the representation as direct product is unique.

This theorem is known as **Fundamental Theorem of Finite Abelian Groups.**

Remarks:

- We know that a cyclic group of order n is isomorphic to $\mathbb{Z}_n$, therefore from the Theorem 9.7, every finite abelian G is isomorphic to a group of the form

$$\mathbb{Z}_{{p_1}^{m_1}} \oplus \mathbb{Z}_{{p_2}^{m_2}} \oplus ... \oplus \mathbb{Z}_{{p_k}^{m_k}}$$

  where $p_i's$ are not necessarily distinct primes and the prime powers ${p_1}^{m_1}, {p_2}^{m_2}, ... , {p_k}^{m_k}$ are uniquely determined by G.

Expressing a group in this form is called determining the isomorphism class of the group.

- If G is a group of order p^k and if k can be written as sum of positive integers $m_1, m_2, \ldots, m_t$, then $\mathbb{Z}_{p^{m_1}} \oplus \mathbb{Z}_{p^{m_2}} \oplus \ldots \oplus \mathbb{Z}_{p^{m_t}}$ is an abelian group of order p^k.
- Let G be a group of order n. Determining groups upto isomorphism of order n means finding all possible non isomorphic groups of order n.
- If $o(G) = n = {p_1}^{m_1} \cdot {p_2}^{m_2} \ldots {p_t}^{m_t}$, $p_i's$ are distinct primes, then number of non–isomorphic abelian groups (or number of abelian groups upto isomorphism) of order n is given by $P(m_1) \cdot P(m_2) \ldots \cdot P(m_t)$.

Corollary 9.3: If G is a finite abelian group having order n and if $m|n$, then G has a subgroup of order m, i.e., the converse of Lagrange's theorem holds for finite abelian groups.

Problem 9.27 Let G be a group of order p^4. Determine all the possible direct products for G.

Solution We have

Partitions of 4	*Possible Direct Product*
4	$\mathbb{Z}p^4$
3 + 1	$\mathbb{Z}p^3 \oplus \mathbb{Z}p$
2 + 2	$\mathbb{Z}p^2 \oplus \mathbb{Z}p^2$
2 + 1 + 1	$\mathbb{Z}p^2 \oplus \mathbb{Z}p \oplus \mathbb{Z}p$
1 + 1 + 1 + 1	$\mathbb{Z}p \oplus \mathbb{Z}p \oplus \mathbb{Z}p \oplus \mathbb{Z}p$

Problem 9.28 Determine upto isomorphism, all abelian groups of order 360.

Solution We have $o(G) = 360 = 2^3 \cdot 3^2 \cdot 5$. Thus, number of abelian groups upto isomorphism $= P(3) \cdot P(2) \cdot P(1) = 3 \cdot 2 \cdot 1 = 6$. They are

$$\mathbb{Z}_{360} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

Problem 9.29 Find the smallest positive integer n such that there are

(i) two non – isomorphic groups of order n,
(ii) three non – isomorphic abelian groups of order n,
(iii) four non – isomorphic abelian groups of order n.

SOLUTION

(i) Let $n = 4$. Then there are two non-isomorphic groups namely, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ of order 4.

(ii) Let $n = 8 = 2^3$. Then there are $P(3) = 3$ non-isomorphic abelian groups of order 8. They are $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

(iii) Let $n = 36 = 2^2 \cdot 3^2$. Then there are $P(2) \cdot P(2) = 2 \cdot 2 = 4$ non-isomorphic abelian groups of order 36. They are $\mathbb{Z}_{36}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

PROBLEM 9.30 How many abelian groups (upto isomorphism) are there of

(i) order 15

(ii) order 42

(iii) order pqr, where p, q, r are distinct primes.

SOLUTION

(i) Let $o(G) = 15 = 3.5$. Then there are $P(1) \cdot P(1) = 1 \cdot 1 = 1$ abelian group of order 15, namely $\mathbb{Z}_{15} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_3$.

(ii) Let $o(G) = 42 = 2 \cdot 3 \cdot 7$. Then there are $P(1) \cdot P(1) \cdot P(1) = 1 \cdot 1 \cdot 1 = 1$ abelian group of order 42, namely $\mathbb{Z}_{42} \cong \mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$.

(iii) Let $o(G) = pqr$. Then there are $P(1) \cdot P(1) \cdot P(1) = 1 \cdot 1 \cdot 1 = 1$ abelian group of order pqr, namely $\mathbb{Z}_{pqr} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$.

PROBLEM 9.31 Let G be an abelian group of order 45. Prove that G has an element of order 15. Does every abelian group of order 45 has an element of order 9?

SOLUTION We have $o(G) = 45 = 3^2 \cdot 5$. Thus $G \cong \mathbb{Z}_{45}$ or $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

The group $\mathbb{Z}_{45}$ has an element namely 3 of order 15. Also, the element $(1, 1, 1) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ has order equal to lcm(3, 3, 5) = 15.

Thus, every abelian group of order 45 has an element of order 15.

The group $\mathbb{Z}_{45}$ has an element namely 5 of order 9. However, the group $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ has no element of order 9 as for no $(a, b, c) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$, we have $o(a, b, c) = \text{lcm}(o(a), a(b), o(c)) = 9$.

PROBLEM 9.32 Let G be an abelian group of order 120 having exactly three elements of order 2. Determine the isomorphism class of G.

SOLUTION We have $o(G) = 120 = 2^3 \cdot 3 \cdot 5$. Thus, number of abelian groups upto isomorphism $= P(3) \cdot P(1) \cdot P(1) = 3 \cdot 1 \cdot 1 = 3$. They are

$$\mathbb{Z}_{120} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

$\mathbb{Z}_8$ has one element namely 4 of order 2, $\mathbb{Z}_4$ has one element 2 of order 2, $\mathbb{Z}_2$ has one element 1 of order 2.

Also, $\mathbb{Z}_3$ and $\mathbb{Z}_5$ have no element of order 2. Then, $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ has an element (4, 0, 0) of order 2 (since $o(4, 0, 0)) = \text{lcm}((2, 1, 1) = 2$).

$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ has three elements namely, (2, 0, 0, 0), (2, 1, 0, 0), (0, 1, 0, 0) of order 2.

Similarly, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ has seven elements of order 2. They are (1, 0, 0, 0, 0), (0, 1, 0, 0, 0), (0, 0, 1, 0, 0), (1, 1, 0, 0, 0), (1, 0, 1, 0, 0), (0, 1, 1, 0, 0), (1, 1, 1, 0, 0).

Therefore, $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Problem 9.33 Determine the isomorphism class of $U(20)$.

Solution We have $o(U(20)) = \varphi(20) = 8 = 2^3$. Thus $U(20)$ is group of order 8 under multiplication modulo 20. Then, the possible isomorphism classes of $U(20)$ are

$$\mathbb{Z}_8$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

We also know that $U(20)$ is not cyclic, so $U(20) \ncong \mathbb{Z}_8$.

Further,

Element	1	3	7	9	11	13	17	19
Order	1	4	4	2	2	4	4	2

Since $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has no element of order 4, so $U(20) \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Hence, $U(20) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$.

Problem 9.34 The set {1, 9, 16, 22, 29, 53, 74, 79, 81} is a group under multiplication modulo 91. Determine the isomorphism class of this group.

Solution We have $o(G) = 9 = 3^2$. The possible isomorphism classes are $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_9$.

Element	1	9	16	22	29	53	74	79	81
Order	1	3	3	3	3	3	3	3	3

Since $\mathbb{Z}_9$ has $\varphi(9) = 6$ elements of order 9 but G has no element of order 9. So $G \ncong \mathbb{Z}_9$. Hence $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$

Problem 9.35 Suppose that the order of some finite abelian group is divisible by 10. Prove that the group has a cyclic subgroup of order 10.

Solution Since the converse of Lagrange's theorem holds for finite abelian groups, so if $10|o(G)$, then G has a subgroup, say K of order 10.

Now $o(K) = 10$, so $K \cong \mathbb{Z}_5 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_{10}$.

Since Z_{10} is cyclic, we have that K is cyclic

Algorithm to express an abelian group G of order p^n as an internal direct product of cyclic groups:

Step 1: Determine the order of all elements of G.

Step 2: Choose an element x_1 of maximal order and define $K_1 = \langle x_1 \rangle$. If $o(G) = o(K_1)$, then we are done.

Step 3: If $o(G) \neq o(K_1)$, then choose an element say x_2 having order less than or equal to $\dfrac{o(G)}{o(K_1)}$ such that no element of $\langle x_2 \rangle$ except identity belongs to the set K_1.

Let $K_2 = \langle x_2 \rangle$. Set $K = K_1 \times K_2$. If $o(K) = o(G)$, then $G = K_1 \times K_2$ and we are done.

Step 4: If $o(G) \neq o(K)$, then repeat step 3 on the set K.

Problem 9.36 Let $G = \{1, 7, 17, 23, 49, 55, 65, 71\}$ be a group under multiplication modulo 96. Write G as an external and internal direct product of cyclic groups.

Solution We have $o(G) = 8 = 2^3$. The possible isomorphism classes are $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_8$.

Element	1	7	17	23	49	55	65	71
Order	1	4	2	4	2	4	2	4

Since $\mathbb{Z}_8$ has $\varphi(8) = 4$ elements of order 8 but G has no element of order 8. So $G \ncong \mathbb{Z}_8$.

Also, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has no element of order 4, so $G \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Hence $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$.

To express G as an internal direct product of cyclic groups, pick an element of maximal order.

Let $H = \langle 7 \rangle = \{1, 7, 49, 55\}$. Next pick an element with order $\dfrac{o(G)}{o(H)} = \dfrac{8}{4} = 2$.

Let $K = \langle 17 \rangle = \{1, 17\}$. Then $H \cap K = \{1\}$ and $G = HK$

Therefore, $G = \langle 7 \rangle \times \langle 17 \rangle$.

PROBLEM 9.37 Let $G = \{1, 7, 43, 49, 51, 57, 93, 99, 101, 107, 143, 149, 151, 157, 193, 199\}$ be a group under multiplication modulo 200. Write G as an external and internal direct product of cyclic groups.

SOLUTION We have $o(G) = 16 = 2^4$. The possible isomorphism classes are

$$\mathbb{Z}_{16}$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_4$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

We now determine the order of each element of G.

Element	1	7	43	49	51	57	93	99	101	107	143	149	151	157	193	199
Order	1	4	4	2	2	4	4	2	2	4	4	2	2	4	4	2

Since G has no element of order 16, so $G \ncong \mathbb{Z}_{16}$. Also G has no element of order 8 whereas $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ has an element (1, 0) of order 8. So, $G \ncong \mathbb{Z}_8 \oplus \mathbb{Z}_2$.

Also, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has no element order 4, while G has eight elements of order 4. So $G \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Now, let $(a, b) \in \mathbb{Z}_4 \oplus \mathbb{Z}_4$. Then $o((a, b)) = 4$ means $\text{lcm}(o(a), o(b)) = 4$.

There are following possibilities:

(i) $o(a) = 4, o(b) = 4$

(ii) $o(a) = 1, o(b) = 4$

(iii) $o(a) = 4, o(b) = 1$

(iv) $o(a) = 4, o(b) = 2$

(v) $o(a) = 2, o(b) = 4$

Thus, total number of elements of order 4 in $\mathbb{Z}_4 \oplus \mathbb{Z}_4 = 4 + 2 + 2 + 2 + 2 = 12$.

But G has eight elements of order 4. So $G \ncong \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Therefore, $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

To express G as an internal direct product of cyclic groups, pick an element of maximal order.

Let $K_1 = \langle 7 \rangle = \{1, 7, 49, 143\}$. Next pick an element with order less than or equal to $\dfrac{o(G)}{o(K_1)} = \dfrac{8}{4} = 2$.

Let $K_2 = \langle 51 \rangle = \{1, 51\}$.

Then $K_1 \cap K_2 = \{1\}$ but $G \neq K_1K_2$ as $o(G) \neq o(K_1K_2) = \dfrac{o(K_1)o(K_2)}{o(K_1 \cap K_2)} = \dfrac{8}{1} = 8$.

Also, $K_1K_2 = \{1, 7, 49, 51, 93, 99, 143, 157\}$.

Let $K_3 = \langle 101\rangle = \{1, 101\}$. Then $K_1K_2 \cap K_3 = \{1\}$ and

$K_1K_2K_3 = \{1, 7, 43, 49, 51, 57, 93, 99, 101, 107, 143, 149, 151, 157, 193, 199\} = G$.

Therefore, $G = \langle 7\rangle \times \langle 51\rangle \times \langle 101\rangle$.

Problem 9.38 Determine the isomorphism class of K_4.

Solution We know K_4 is an abelian group of order 4.

Now $o(K_4) = 2^2$. Thus, the abelian groups upto isomorphism of order 4 are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Since K_4 has no element of order 4 whereas $\mathbb{Z}_4$ has $\varphi(4) = 2$ elements of order 4. So $K_4 \ncong \mathbb{Z}_4$.

Therefore, $K_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Problem 9.39 Let G be a group of order 108. Show that

(i) there are two abelian groups of order 108 upto isomorphism that have exactly one subgroup of order 3.

(ii) there are two abelian groups of order 108 upto isomorphism that have exactly four subgroups of order 3.

(iii) there are two abelian groups of order 108 upto isomorphism that have exactly thirteen subgroups of order 3.

Solution We have $o(G) = 108 = 2^2 \cdot 3^3$. The number of abelian groups upto isomorphism is $P(2) \cdot P(3) = 2 \cdot 3 = 6$. They are

$$\mathbb{Z}_{108} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{27}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

To find the number of subgroups of order 3, we need to first find the number of elements of order 3.

The groups $\mathbb{Z}_4$ and $\mathbb{Z}_2$ have no elements of order 3. So, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ have no element of order 3.

We will now find the number of elements of order 3 in $\mathbb{Z}_{27}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_9$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Consider the following table:

Group	*Element*	*Possible orders*	*No. of elements*
$\mathbb{Z}_{27}$	a	$o(a) = 3$	$\varphi(3) = 2$
$\mathbb{Z}_3 \oplus \mathbb{Z}_9$	(a, b)	$o(a) = 3, o(b) = 1$	$\varphi(3) \cdot \varphi(1) = 2$
		$o(a) = 1, o(b) = 3$	$\varphi(1) \cdot \varphi(3) = 2$
		$o(a) = 3, o(b) = 3$	$\varphi(3) \cdot \varphi(3) = 4$
$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$	(a, b, c)		$3^3 - 1 = 26$ (Since each a, b, c has three choices namely 0, 1, 2 but (0, 0, 0) is excluded as its order is 1.)

The number of subgroups of order 3 in $\mathbb{Z}_{27}$.

$$= \frac{\text{number of elements of order 3 in } \mathbb{Z}_{27}}{\text{number of elements of order 3 in one cyclic subgroup of order 3} = \varphi(3)}$$

$$= \frac{2}{2} = 1$$

Thus, the number of subgroups of order 3 in $\mathbb{Z}_4 \oplus \mathbb{Z}_{27}$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27}$ is one.

Similarly, the number of subgroups of order 3 in $\mathbb{Z}_3 \oplus \mathbb{Z}_9 = \frac{8}{2} = 4$.

Therefore, the number of subgroups of order 3 in $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$ is four.

Also, the number of subgroups of order 3 in $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 = \frac{26}{} = 13$.

Therefore, the number of subgroups of order 3 in $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ is thirteen.

EXERCISES

1. Find all cyclic subgroups of order 10 in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$.
2. Express $U(105)$ as an external direct product of cyclic additive groups of the form $\mathbb{Z}_n$.
3. Find the number of elements of order six in $\text{Aut}(\mathbb{Z}_{720})$.
4. Prove that $\mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.
5. Prove that $\text{Aut}(\mathbb{Z}_{125})$ is a cyclic group.
6. Prove that $D_3 \oplus D_4$ is not isomorphic to D_{24}.
7. Show that S_3 cannot be expressed as an internal direct product of two non-trivial subgroups.

8. If the order of some finite abelian group is divisible by 4, show by example, the group need not have a cyclic subgroup of order 4.

9. Determine the isomorphism class of $U(100)$. How many elements of order 20 does $U(100)$ have?

10. Let $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ be a group under multiplication modulo 65. Write G as an external and internal direct product of cyclic groups.

Hints to Selected Problems

1. In order to find the number of cyclic subgroups of order 10, we first need to find the number of elements of order 10.

Let $(a, b) \in \mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$, then $\text{lcm}(o(a), o(b)) = 10$ gives the following possibilities:

(i) $o(a) = 10, o(b) = 1$, (ii) $o(a) = 10, o(a) = 5$, (iii) $o(a) = 2, o(b) = 5$.

This gives that there are 24 elements of order 10 in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$. And thus there are six subgroups of order 10 in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$.

3. We have $\text{Aut}(\mathbb{Z}_{720}) \cong U(270) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_4$.

Let $(a, b, c, d) \in \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_4$ then $\text{lcm}(o(a), o(b), o(c), o(d)) = 6$ gives that there are 30 elements of order 6 in $\text{Aut}(\mathbb{Z}_{720})$.

10. $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$ and $G = \langle 8 \rangle \times \langle 12 \rangle$.

❑❑❑

Check for updates

10

Group Actions

Learning Objectives

- Group Actions.
- Generalized Cayley's Theorem.
- Conjugate Classes and Conjugacy in S_n.

10.1 Group Actions

We outline group action and substantiate with various examples. Group action is a potent tool which can be employed to gain insight into the structure of groups. It is a representation of the elements of a group as symmetries of a set. Many groups have a natural group action coming from their construction; e.g. the dihedral group D_4 acts on the vertices of a square because the group is given as a set of symmetries of the square. A group action of a group on a set is a generalization of this idea, which can be used to derive useful facts about both the group and the set it acts on.

Definition 10.1: Let A be a set and let G be a group. A **group action** of G on A is a map $*$ from $G \times A$ to A denoted by $(g, a) \to g * a$ satisfying the following properties:

1. $g_1 * (g_2 * a) = (g_1 g_2) * a$ for all $a \in A$, $g_1, g_2 \in G$
2. $e * a = a$ for all $a \in A$, where e is the identity element of G.

Here A is called a G – set and we say that G acts on A.

Example

1. Let G be a group and let A be a non-empty set. Define a map $*$ from $G \times A$ to A by $g * a = a$ for all $g \in G$ and $a \in A$. Then

   $g_1 * (g_2 * a) = a = (g_1 g_2) * a$ and $e * a = a$ for all $a \in A$.

   Thus, $*$ defines a group action on the set A. This action is called the **trivial action** and we say that G acts trivially on A.

© The Author(s) 2023
D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_10

2. Let G be a group and let $A = G$. Define a map $*$ from $G \times A$ to A by $g * a = ga$ for all $g \in G$ and $a \in A$. Then

   (i) $g_1 * (g_2 * a) = g_1 * (g_2 a) = g_1(g_2 a) = (g_1 g_2)a = (g_1 g_2) * a$

   (ii) $e * a = ea = a$ for all $a \in A$.

   Thus, $*$ defines a group action of G on itself. This action is called the **action by left multiplication** or **left regular action** of G on itself.

3. Let $G = (\mathbb{Z}, +)$ and let $A = G$. Define a map $* : G \times A \to A$ by $g * a = g + a$ for all $g \in G$ and $a \in A$. Then $*$ defines a group action of G on itself as

   (i) $g_1 * (g_2 * a) = g_1 * (g_2 + a) = g_1 + (g_2 + a) = (g_1 + g_2) + a$
   $= (g_1 + g_2) * a$

   (ii) $e * a = e + a = a$ for all $a \in A$.

4. Let G be a group and let $A = G$. Define a map from $G \times A$ to A by $g * a = ag^{-1}$ for all $g \in G$ and $a \in A$. Then

   (i) $g_1 * (g_2 * a) = g_1 * (ag_2^{-1}) = (ag_2^{-1})g_1^{-1} = a(g_1 g_2)^{-1} = (g_1 g_2) * a$

   (ii) $e * a = ae^{-1} = a$ for all $a \in A$.

   Thus, $*$ defines a group action of G on itself. This action is called the **action from right by multiplication** or **by translation** of G on itself.

5. Let G be a group and let $A = G$. Define a map $*$ from $G \times A$ to A by $g * a = gag^{-1}$ for all $g \in G$ and $a \in A$. Then

   (i) $g_1 * (g_2 * a) = g_1 * (g_2 a g_2^{-1}) = g_1(g_2 a g_2^{-1})g_1^{-1}$
   $= (g_1 g_2)a(g_1 g_2)^{-1} = (g_1 g_2) * a$

   (ii) $e * a = eae^{-1} = a$ for all $a \in A$.

   Thus, $*$ defines a group action of G on itself. This action is called the **action by conjugation** of G on itself.

6. Let G be a group and H be a subgroup of G. Let A be the set of all left cosets of H in G.

   Define $* : G \times A \to A$ by $g * aH = gaH$ for all $g \in G$ and $aH \in A$. Then,

   (i) $g_1 * (g_2 * aH) = g_1 * (g_2 aH) = g_1 g_2 aH = (g_1 g_2) * aH$

   (ii) $e * aH = eaH = aH$ for all $aH \in A$.

   Thus, G acts on the set of all left cosets of a subgroup H of G.

7. Let H be a normal subgroup of a group G and let $A = G/H$, the set of all left cosets of H in G.

   Define $* : G \times A \to A$ by $g * aH = gag^{-1}H$ for all $g \in G$ and $aH \in A$. Then,

   (i) $g_1 * (g_2 * aH) = g_1 * (g_2 a g_2^{-1} H) = g_1(g_2 a g_2^{-1})g_1^{-1}H$
   $= (g_1 g_2)a(g_1 g_2)^{-1}H$
   $= (g_1 g_2) * aH$

(ii) $e * aH = eae^{-1}H = aH$ for all $aH \in A$.

Thus, $*$ defines a group action and thus G/H is a G – set.

8. Let $G = (\mathbb{R}, +)$ and let $A = \mathbb{R} \times \mathbb{R}$. Define a map $* : G \times A \to A$ by $g * (x, y) = (x + gy, y)$. Then,

(i) $g_1 * (g_2 * (x, y)) = g_1 * (x + g_2y, y) = (x + g_2y + g_1y, y)$

$= (x + (g_1 + g_2)y, y)$

$= (g_1 + g_2) * (x, y)$

(ii) $0 * (x, y) = (x + 0y, y) = (x, y)$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$.

Thus, $*$ defines a group action.

Theorem 10.1: Let G be group and let A be a non-empty set. Then any homomorphism from G to S_A, the symmetric group of A, defines a group action of G on A.

Conversely, any group action of G on A induces a homomorphism from G to S_A.

Proof: Let $\theta : G \to S_A$ be any homomorphism. Then, for any $g \in G$, let $\theta(g) = \sigma_g$, where $\sigma_g : A \to A$ is a permutation.

Then as θ is a homomorphism we have, $\theta(ab) = \sigma_{ab} = \sigma_a\sigma_b = \theta(a)\,\theta(b)$.

Define a map $* : G \times A \to A$ by $g * a = \sigma_g(a)$, $a \in A$, $g \in G$.

Then, $g_1 * (g_2 * a) = g_1 * (\sigma_{g_2}(a)) = \sigma_{g_1}(\sigma_{g_2}(a)) = \sigma_{g_1}\sigma_{g_2}(a) = \sigma_{g_1g_2}(a)$

$= (g_1g_2) * a$

Also, $e * a = \sigma_e(a) = I(a) = a$ for all $a \in A$.

Thus, G acts on A.

Conversely, let $*$ be a group action of G on A. Define a mapping $\varphi : G \to S_A$ by $\varphi(g) = \sigma_g$, where $\sigma_g : A \to A$ such that $\sigma_g(x) = g * x$.

We first show that σ_g is a permutation on A. For this we need to prove that σ_g is a one–one, onto map from A to A. Now,

$$\sigma_g(x) = \sigma_g(y)$$

$$\Rightarrow \quad g * x = g * y$$

$$\Rightarrow \quad g^{-1} * (g * x) = g^{-1} * (g * y)$$

$$\Rightarrow \quad (g^{-1}g) * x = (g^{-1}g) * y$$

$$\Rightarrow \quad e * x = e * y$$

Thus, $x = y$ and so σ_g is one–one.

Let $y \in A$ be any element, then as $* : G \times A \to A$ is a group action, for $y \in A$, $g \in G$ we have $g^{-1} * y \in A$ such that

$$\sigma_g(g^{-1} * y) = g * (g^{-1} * y) = (gg^{-1}) * y = e * y = y$$

Thus, σ_g is onto and hence $\sigma_g \in S_A$.

We now show that φ is a homomorphism.

Let $a, b \in G$ and $x \in A$ be any elements. Then,

$$\sigma_{ab}(x) = (ab) * x = a * (b * x) = \sigma_a(\sigma_b(x)) = \sigma_a\sigma_b(x)$$

Therefore, $\sigma_{ab} = \sigma_a\sigma_b$ and hence $\varphi(ab) = \varphi(a)\,\varphi(b)$.

Thus φ is a homomorphism. The mapping φ is called the **permutation representation** of G associated to the given group action.

EXAMPLE:

1. Let G be a group acting trivially on a non-empty set A. Let φ be the associated permutation representation, then $\varphi : G \to S_A$ such that
   $\varphi(g) = \sigma_g$, where $\sigma_g : A \to A$ such that $\sigma_g(x) = g * x = x$.
   Then $\sigma_g(x) = x = \sigma_e(x)$ for all $x \in A$. Thus, $\sigma_g = \sigma_e = I$.
   Therefore, the associated permutation representation φ is the trivial homomorphism that maps every element of G to the identity permutation.

   As a corollary to this theorem, we provide the proof of the well-known **Cayley's Theorem**.

COROLLARY 10.1: Every group is isomorphic to a permutation group.

This can also be restated as: If G is a group of order n then G is isomorphic to a subgroup of S_n.

Proof: Let G be any group and let $A = G$. Define $* : G \times A \to A$ by $g * a = ga$. Then we have that G acts on A by left multiplication. Therefore, from the theorem there exists a homomorphism,

$$\varphi : G \to S_A \text{ such that } \varphi(g) = \sigma_g,$$

where $\sigma_g : A \to A$ given by $\sigma_g(x) = g * x = gx$.

We now show that φ is one–one.

$$\varphi(g_1) = \varphi(g_2) \Rightarrow \sigma_{g_1} = \sigma_{g_2} \Rightarrow \sigma_{g_1}(a) = \sigma_{g_2}(a) \text{ for all } a \in A$$

$$\Rightarrow \quad \sigma_{g_1}(e) = \sigma_{g_2}(e)$$

$$\Rightarrow \quad g_1 e = g_2 e$$

Thus, $g_1 = g_2$ and hence φ is one–one. Thus $\ker\varphi = \{e\}$

Therefore, by fundamental theorem of homomorphism, $G \cong \varphi(G)$, a subgroup of $S_A (= S_G)$

COROLLARY 10.2: Let G be a group acting on itself by conjugation, then $\dfrac{G}{Z(G)} \cong \text{Inn}(G)$.

Proof: Since G acts on itself by conjugation, there exists a homomorphism

$$\varphi : G \to S_A \text{ such that } \varphi(g) = \sigma_g,$$

where $\sigma_g : A \to A$ given by $\sigma_g(x) = g * x = gxg^{-1}$.

By Fundamental theorem of homomorphism, $\frac{G}{\text{Ker}\,\varphi} \cong \varphi(G)$.

Now, $\ker\varphi = \{g \in G : \varphi(g) = I\} = \{g \in G : \sigma_g = I = \sigma_e\}$

$= \{g \in G : \sigma_g(a) = \sigma_e(a) \ \forall \ a \in A\}$

$= \{g \in G : gag^{-1} = eae^{-1}\}$

$= \{g \in G : ga = ag\} = Z(G)$

Also, $\varphi(G) = \{\sigma_g \in S_A : \sigma_g(a) = gag^{-1}\} = \text{Inn}(G)$.

Thus, we have $\frac{G}{Z(G)} \cong \text{Inn}(G)$.

Problem 10.1 Let G be a group and let $A = G$. Show that if G is non-abelian then the map defined by $g * a = ag$ for all $g, a \in G$ is not a group action of G on itself.

Solution Since G is non- abelian, there exist some $g_1, g_2 \in G$ such that $g_1g_2 \neq g_2g_1$.

Now, $g_1 * (g_2 * a) = g_1 * (ag_2) = (ag_2)g_1 = a(g_2g_1) \neq a(g_1g_2) = (g_1g_2) * a$

Thus, $*$ is not a group action.

10.2 Kernels, Orbits and Stabilizers

Definition 10.2: Let A be a set and let G be a group acting on A. Then the **Kernel of the action** of G on A is the set of elements of G which fixes all the elements of A.

i.e., $\text{Ker} = \{g \in G : g * a = a \ \text{ for all } a \in A\}$

Example:

1. Let G be a group acting trivially on the set A, then
$$\text{Ker} = \{g \in G : g * a = a \ \text{ for all } a \in A\} = G$$
2. Let G be a group acting on the set $A = G$ by left multiplication, then
$$\text{Ker} = \{g \in G : g * a = a \ \text{ for all } a \in A\}$$
$$= \{g \in G : ga = a \ \text{ for all } a \in A\}$$
$$= \{g \in G : g = e\} = \{e\}$$
3. Let G be a group acting on itself by conjugation, then the kernel of the action is
$$\text{Ker} = \{g \in G : g * a = a \ \text{ for all } a \in A\}$$
$$= \{g \in G : gag^{-1} = a \ \text{ for all } a \in A\}$$
$$= \{g \in G : ga = ag \text{ for all } a \in A\} = Z(G)$$

Theorem 10.2: Let $* : G \times A \to A$ be a group action, then Kernel of this action forms a subgroup of G.

Proof:

We have, Ker $= \{g \in G : g * a = a \text{ for all } a \in A\}$

Since, $e * a = a$ for all $a \in A$, we have $e \in$ Ker and so Ker is non empty.

Now let $x, y \in$ Ker, then $x * a = a$ and $y * a = a$ for all $a \in A$.

Thus, $(xy) * a = x * (y * a) = x * a = a$ for all $a \in A$ and so $xy \in$ Ker.

Also, $x \in$ Ker $\Rightarrow$ $x * a = a$ for all $a \in A$

$\Rightarrow$ $x^{-1} * (x * a) = x^{-1} * a$ for all $a \in A$

$\Rightarrow$ $(x^{-1}x) * a = x^{-1} * a$ for all $a \in A$

$\Rightarrow$ $e * a = x^{-1} * a$ for all $a \in A$

$\Rightarrow$ $a = x^{-1} * a$ for all $a \in A$

Thus, $x^{-1} \in$ Ker.

Therefore, Kernel of the action is a subgroup of G.

Problem 10.2 Let G be a group and let A be a non-empty set such that G acts on A. Show that the Kernel of an action of G on A is same as the Kernel of the corresponding permutation representation $\varphi : G \to S_A$.

Solution Let $* : G \times A \to A$ be a group action and let $\varphi : G \to S_A$ be the associated permutation representation, then φ is a homomorphism.

Now, ker $\varphi = \{g \in G : \varphi(g) = I\}$

$= \{g \in G : \sigma_g = I\}$

$= \{g \in G : \sigma_g(a) = I(a) \text{ for all } a \in A\}$

$= \{g \in G : g * a = a \text{ for all } a \in A\}$ = Kernel of group action.

Remark: The Kernel of group action being equal to kernel of group homomorphism, is a normal subgroup of G.

Definition 10.3: Let A be a set and let G be a group acting on A. We say that action of G on A is **faithful** if only the identity element of G fixes every element of A, i.e., if distinct elements of G induce distinct permutations of A.

Problem 10.3 Prove that an action is faithful if and only if the associated permutation representation φ is one–one, i.e., ker $\varphi = \{e\}$.

Solution Let $* : G \times A \to A$ be a group action which is faithful, then $g * a = a$ only when $g = e$.

Now, Ker = $\{g \in G : g * a = a \text{ for all } a \in A\} = \{e\}$ and we know that kernel of an action is same as ker φ.

Thus, Ker φ = $\{e\}$ and so φ is one–one.

Otherway, let φ be one–one. Then, ker φ = $\{e\}$ and so Ker = $\{e\}$. Thus, only identity element fixes every element of A and hence the action is faithful.

EXAMPLE:

1. Since the kernel of trivial action is G, therefore trivial action is not faithful.
2. Since the kernel of action by left multiplication is $\{e\}$. So, the action is faithful.
3. We have if G acts on itself by conjugation, then the action is faithful only when the centre of G is $\{e\}$.
4. Let $G = D_4$ acts on the set $A = \{1, 2, 3, 4\}$ in clockwise manner. Let x denotes the rotation of the square clockwise by 90° and let y denotes the reflection about the line passing through the vertices 1 and 3. Then, $\sigma_x = (1234)$ and $\sigma_y = (24)$. Since corresponding to every action of G on A, there is a associated permutation representation which is a homomorphism, so $\sigma_{yx} = \sigma_y\sigma_x = (14)(23)$.

   Also, since identity permutation fixes every element of A, so the action of G on A is faithful.

PROBLEM 10.4 Let G be a group acting on a non-empty set A under $*$. For any $a, b \in A$, define $a \sim b$ if and only if there exists some $g \in G$ such that $a = g * b$, then show that ~ is an equivalence relation.

SOLUTION Since $a = e * a$ for all $a \in A$, so $a \sim a$ and thus reflexivity holds. For symmetry, assume that $a \sim b$ then there exists some $g \in G$ such that $a = g * b$.

This gives $g^{-1} * a = g^{-1} * (g * b) = (g^{-1}g) * b = e * b = b$.

Therefore, $b \sim a$.

Let $a \sim b$ and $b \sim c$, then there exist $g_1, g_2 \in G$ such that $a = g_1 * b$ and $b = g_2 * c$.

Then, $a = g_1 * b = g_1 * (g_2 * c) = (g_1g_2)*c$ and so $a \sim c$. Thus, transitivity holds.

Therefore, ~ is an equivalence relation.

The equivalence class corresponding to this equivalence relation is called the Orbit.

DEFINITION 10.4: Let $a \in A$ be any element, then equivalence class of a is given by

$$cl(a) = \{x \in A : x \sim a\} = \{x \in A : x = g * a \text{ for some } g \in G\}$$
$$= \{g * a : g \in G\}$$

This is called the **orbit of *G* containing *a*** and is denoted by $\mathcal{O}_a$.

Therefore, $\mathcal{O}_a = \{g * a : g \in G\}$

Thus, a group G acting on a non-empty set A leads to a partition of A into disjoint equivalence classes under the action of G on A and these equivalence classes are called the Orbits of elements of A. So, A can be expressed as a union of these distinct orbits of elements of A.

Example:

1. Let $*$ be a trivial action, then the orbit of any $a \in A$ is given by
$$\mathcal{O}_a = \{g * a : g \in G\} = \{a\}$$
2. Let G acts on A by left multiplication, then the orbit of $a \in A$ is given by
$$\mathcal{O}_a = \{g * a : g \in G\} = \{ga : g \in G\} = G.$$

Problem 10.5 Let G be a finite group and let H be a subgroup of G. Suppose H acts on G by left multiplication. Let $x \in G$ and let $\mathcal{O}_x$ be the orbit of x under the action of H on G. Prove that the mapping $\varphi : H \to \mathcal{O}_x$ defined by $\varphi(h) = h * x = hx$ is one -one and onto. Also, deduce Lagrange's Theorem.

Solution We have,
$$h_1 = h_2 \Leftrightarrow h_1x = h_2x \Leftrightarrow \varphi(h_1) = \varphi(h_2)$$

Thus φ is well- defined and one–one.

Also, φ is onto. Thus φ is a bijection and hence $o(H) = o(\mathcal{O}_x)$.

Therefore, order of each orbit is equal to the order of H. Since orbits of elements of G partitions G into equivalence classes, we have
$$G = \mathcal{O}_1 \cup \mathcal{O}_2 \cup ... \cup \mathcal{O}_t$$
where $\mathcal{O}_i$ are distinct orbits in G.

Thus, $o(G) = o(\mathcal{O}_1) + o(\mathcal{O}_2) + ... + o(\mathcal{O}_t) = \underbrace{o(H) + o(H) + ... + o(H)}_{t \text{ times}} = t \cdot o(H)$

Therefore, $o(H) | o(G)$ and hence the Lagrange's theorem.

Definition 10.5: Let G be a group acting on a non-empty set A. Let $a \in A$ be a fixed element, then the **stabilizer** of a in G is given by the set
$$G_a = \{g \in G : g * a = a\}$$

Example:

1. Let $*$ be a trivial action, and let $a \in A$ be any element then the stabilizer of a in G is given by
$$G_a = \{g \in G : g * a = a\} = G.$$

Theorem 10.3: Let G be a group acting on a non-empty set A and let $a \in A$ be fixed. Then G_a, the stabilizer of a in G, is a subgroup of G.

Proof: We have, $G_a = \{g \in G : g * a = a\}$. Since $e * a = a$, so $e \in G_a$ and hence G_a is non-empty.

Now let $x, y \in G_a$, then $x * a = a$ and $y * a = a$.

Therefore, $(xy) * a = x * (y * a) = x * a = a$, so $xy \in G_a$.

Also, $a = e * a = (x^{-1}x) * a = x^{-1} * (x * a) = x^{-1} * a$. Thus, $x^{-1} \in G_a$.

Therefore, G_a is a subgroup of G.

Remark: By definition of Kernel of a group action and stabilizers of elements of A, we observe that Kernel of group action is the intersection of the stabilizers of all the elements of A.

We now prove the well-known **Orbit–Stabilizer Theorem.**

Theorem 10.4: Let G be a group acting on a non- empty set A. Let $a \in A$, then

$$o(G) = o(\mathcal{O}_a)o(G_a)$$

Proof: Let G/G_a denotes the set of all left cosets of G_a in G.

Define a map $\varphi : \mathcal{O}_a \to G/G_a$ by $\varphi(g * a) = gG_a$, $g \in G$. Then,

$$\begin{aligned}
& g_1 * a = g_2 * a \\
\Leftrightarrow \quad & {g_1}^{-1} * (g_1 * a) = {g_1}^{-1} * (g_2 * a) \\
\Leftrightarrow \quad & ({g_1}^{-1}g_1) * a = ({g_1}^{-1}g_2) * a \\
\Leftrightarrow \quad & a = ({g_1}^{-1}g_2) * a \\
\Leftrightarrow \quad & {g_1}^{-1}g_2 \in G_a \\
\Leftrightarrow \quad & g_1G_a = g_2G_a \\
\Leftrightarrow \quad & \varphi(g_1 * a) = \varphi(g_2 * a)
\end{aligned}$$

Thus, φ is well–defined and one-one.

Also, since for any $gG_a \in G/G_a$, there exists $g * a \in \mathcal{O}_a$ such that $\varphi(g * a) = gG_a$ and so φ is onto.

Thus φ is a bijection and hence $o(\mathcal{O}_a) = o(G/G_a) = \dfrac{o(G)}{o(G_a)}$ = index of G_a in G.

Therefore, $o(G) = o(\mathcal{O}_a) \cdot o(G_a)$.

Definition 10.6: Let G be a group acting on a non-empty set A. The action of G on A is called **transitive** if there is only one orbit, i.e., given any two elements a, $b \in A$, there is some $g \in G$ such that $a = g * b$.

Problem 10.6 Let $A = \{1, 2, 3\}$ and let $G = S_3$. Define $* : G \times A \to A$ by $\sigma * a = \sigma(a)$ for all $a \in A$. Show that G acts on A. Find the orbit and stabilizer of each element of A. Prove that the action of G on A is transitive.

Solution We have,

$\sigma_1 * (\sigma_2 * a) = \sigma_1 * (\sigma_2(a)) = \sigma_1(\sigma_2(a)) = (\sigma_1\sigma_2)(a) = (\sigma_1\sigma_2) * a$

and $I * a = I(a) = a$ for all $a \in A$.

Therefore, G acts on A.

Now for any $a \in A$, $G_a = \{g \in G : \sigma * a = a\} = \{g \in G : \sigma(a) = a\}$.

Thus, $G_1 = \{g \in G : \sigma(1) = 1\} = \{I, (23)\}$.

Similarly, $G_2 = \{I, (13)\}$ and $G_3 = \{I, (12)\}$.

Since $o(G) = o(\mathcal{O}_a)o(G_a)$, we have $o(G) = o(\mathcal{O}_1)o(G_1)$.

Thus, $o(\mathcal{O}_1) = \dfrac{o(G)}{o(G_1)} = \dfrac{6}{2} = 3$. Also since $\mathcal{O}_1 \subseteq A$ and $o(A) = 3$, we have $\mathcal{O}_1 = A$.

Similarly, it can be seen that $\mathcal{O}_2 = \mathcal{O}_3 = A$.

Thus, there exists only one orbit and so the action of G on A is transitive.

Problem 10.7 Let $A = \{1, 2, \ldots, n\}$ and let $G = S_n$ be a group acting on the set A by $g * a = g(a)$ for all $a \in A$. Prove that the action of G on A is faithful and show that for each $i \in A$, $G_i \cong S_{n-1}$.

Solution Let $\tau \in G$ be such that $\tau(i) = i$ for all $i \in A$. Then $\tau = I$ and so the action of G on A is faithful.

Now, let $B = A\backslash\{i\}$ and define a map $f : G_i \to S_B$ by $f(\sigma) = \sigma|_B$.

Since $\sigma \in G_i$, so σ fixes i and permutes the remaining elements of A. Thus, $\sigma|_B \in S_B$ and so the mapping is well-defined.

Let $\rho, \sigma \in G_i$ be such that $f(\rho) = f(\sigma)$, then, $\rho|_B = \sigma|_B$.

Thus, $\rho(b) = \sigma(b)$ for all $b \in B$. Also $\rho(i) = \sigma(i) = i$ and therefore, we have, $\rho(a) = \sigma(a)$ for all $a \in A$.

Thus $\rho = \sigma$ and hence f is one-one.

Now let $\tau \in S_B$ be any element, then τ can be extended to $\tau' : A \to A$ by defining $\tau'(i) = i$ and $\tau'(x) = \tau(x)$ for all $x \in B$.

Thus, $\tau' \in S_A$ and $\tau' = \tau|_B$ and so $f(\tau') = \tau$.

Hence f is onto.

For any $\rho, \sigma \in G_i$, $f(\rho\sigma) = (\rho\sigma)|_B = \rho|_B \cdot \sigma|_B = f(\rho)\, f(\sigma)$.

Thus f is a homomorphism and hence an isomorphism.

Therefore, $G_i \cong S_B = S_{n-1}$.

Problem 10.8 Let $A = \{1, 2, \ldots, n\}$ and let $G = S_n$ be a group acting on the set A by $g * a = g(a)$ for all $a \in A$. Prove that the action of G on A is transitive.

Solution We have, $o(G) = o(S_n) = n!$. Let $a \in A$ be any element then,

$$G_a = \{g \in G : g * a = a\}$$

Thus, $G_1 = \{\tau \in S_n : \tau * 1 = 1\} = \{\tau \in S_n : \tau(1) = 1\}$

$$= \{I, (2\ 3), \ldots, (n\ n-1)\ (n\ n-2)\}$$

Thus, G_1 is the set of all those elements of S_n that fixes 1 and permutes rest of the elements. So, $o(G_1) = (n-1)!$.

Similarly, we can find $G_2, G_3, \ldots, G_n$.

Also, $o(G) = o(\mathcal{O}_1) \cdot o(G_1) \Rightarrow n! = o(\mathcal{O}_1) \cdot (n-1)!$

Thus, $o(\mathcal{O}_1) = n = o(A)$. So, $\mathcal{O}_1 = A$.

Similarly, it can be seen that $\mathcal{O}_2 = \mathcal{O}_3 = \ldots = \mathcal{O}_n = A$. Since there is only one orbit, the action is transitive.

Problem 10.9 Let $A = \{1, 2, 3, 4\}$ and let $G = D_4$ be a group acting on the set A by $g * a = g(a)$ for all $a \in A$. Prove that the action of G on A is transitive and verify the Orbit–Stabilizer theorem.

Solution We have, $\mathcal{O}_1 = \{g * 1 : g \in D_4\} = \{g(1) : g \in D_4\}$

$$= \{R_0(1), R_{90}(1), R_{180}(1), R_{270}(1), F_H(1), F_V(1), F_D(1), F_{D'}(1)\}$$

$$= \{1, 2, 3, 4, 4, 2, 3, 1\} = \{1, 2, 3, 4\} = A$$

Thus, $o(\mathcal{O}_1) = 4$.

Similarly, $\mathcal{O}_2 = \mathcal{O}_3 = \mathcal{O}_4 = A$. Since there is only one orbit, the action is transitive.

Also, $G_1 = \{g \in D_4 : g * 1 = 1\}. = \{R_0, F_{D'}\}$. Thus, $o(G_1) = 2$.

Therefore, $o(\mathcal{O}_1) \cdot o(G_1) = 4.2 = 8 = o(G)$

Similarly, we can verify the theorem for the vertices 2, 3, 4 of the square.

Problem 10.10 Let G be a group acting trivially on a non-empty set A. Then the action of G on A is transitive if and only if $o(A) = 1$.

Solution We know that if the action of G on A is trivial then, $G_a = G$ and $\mathcal{O}_a = \{a\}$ for all $a \in A$.

Now, let $* : G \times A \to A$ be transitive, then there is only one orbit say, $\mathcal{O}_x$ and under trivial action, that orbit is of the form $\{x\}$. Thus $A = \{x\}$ and so $o(A) = 1$.

Otherway, let $o(A) = 1$, then $A = \{a\}$ and in trivial action any orbit is of the form $\{a\}$, and so there exists only one orbit.

Thus, the action is transitive.

Problem 10.11 Let G be a group acting transitively on a non-empty set A. Then a subgroup of G need not be transitive on A.

Solution Let $G = S_4$ be a group acting on the set $A = \{1, 2, 3, 4\}$. For any two elements $i, j \in A$, the transposition $\sigma = (i\ j)$ of S_4 maps i to j. Thus G is transitive on A.

Now, let $H = \{I, (1\ 2)(3\ 4)\}$. Then H is a subgroup of G but there is no element in H that maps 1 to 3. Thus H is not transitive on A.

Problem 10.12 Let G be a group acting on a non-empty set A. Prove that if $a, b \in A$ and $b = g * a$ for some $g \in G$, then $G_b = gG_ag^{-1}$. Also, deduce that if the action of G on A is transitive then $\ker = \bigcup_{g \in G} gG_ag^{-1}$.

Solution We have, $x \in G_b \Leftrightarrow b = x * b$

$\Leftrightarrow g * a = x * (g * a)$

$\Leftrightarrow g * a = (xg) * a$

$\Leftrightarrow a = (g^{-1}xg) * a$

$\Leftrightarrow g^{-1}xg \in G_a$

$\Leftrightarrow x \in gG_ag^{-1}$

Thus, $G_b = gG_ag^{-1}$

Since G acts on A transitively, so for a fixed $a \in A$, the orbit of a is given by $\mathcal{O}_a = \{g * a : g \in G\} = A$.

Since there is only one orbit, given any $x \in A$, it must belong to $\mathcal{O}_a$ and so $x = g * a$ for some $g \in G$.

Also, we know $\text{Ker} = \bigcap_{x \in A} G_x = \bigcap_{g \in G} G_{g*a} = \bigcap_{g \in G} gG_ag^{-1}$.

Problem 10.13 Let G be a permutation group on a set A. Let $\sigma \in G$ and let $a \in A$ then prove that $G_{\sigma(a)} = \sigma G_a\sigma^{-1}$. Also, deduce that if the action of G on A is transitive then $\bigcap_{\sigma \in G} \sigma G_a\sigma^{-1} = \{I\}$.

Solution We have, $x \in G_{\sigma(a)}$

$\Leftrightarrow \sigma(a) = x * \sigma(a)$

$\Leftrightarrow \sigma * a = x * (\sigma * a)$

$\Leftrightarrow \sigma * a = (x\sigma) * a$

$\Leftrightarrow a = (\sigma^{-1}x\sigma) * a$

$\Leftrightarrow \sigma^{-1}x\sigma \in G_a$

$\Leftrightarrow x \in \sigma G_a\sigma^{-1}$

Thus, $G_{\sigma(a)} = \sigma G_a\sigma^{-1}$.

Since in a permutation group S_A, only identity permutation fixes every element of A, so Kernel of the action of G on A consists only of identity permutation.

Thus, $\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \bigcap_{\sigma \in G} G_{\sigma(a)} = \text{Ker} = \{I\}$.

Problem 10.14 Let G be an abelian, transitive subgroup of S_A, show that $\sigma(a) \neq a$ for all $\sigma \neq I$ and all $a \in A$. Also, deduce that $o(G) = o(A)$.

Solution We have from above question, $\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \{I\}$.

Since G is abelian, $\bigcap_{\sigma \in G} G_a = \{I\}$ and so $G_a = \{I\}$ for all $a \in A$.

Thus, for all $a \in A$ and $\sigma \neq I$, we have $\sigma(a) \neq a$.

Now, let $a \in A$ be fixed and $f : G \to A$ be defined by $f(\sigma) = \sigma(a)$.

We will show that f is one-one and onto.

Let $\sigma, \tau \in G$ be such that $f(\sigma) = f(\tau)$.

$\Rightarrow \quad \sigma(a) = \tau(a)$

$\Rightarrow \quad \tau^{-1}\sigma(a) = a$

So, $\tau^{-1}\sigma \in G_a = \{I\}$ and thus, $\sigma = \tau$. Hence f is one-one.

Also, since G is transitive, for all $b \in A$, $b = \sigma(a)$, for some $\sigma \in G$ and thus, f is onto.

Hence f is a bijection and so $o(G) = o(A)$.

Theorem 10.5: Every element of S_n can be expressed as product of disjoint cycles. The expression is unique except for the order of the cycles.

Proof: Let $A = \{1, 2, \ldots, n\}$ and let $\sigma \in S_n$ be any permutation.

Let $G = \langle \sigma \rangle = \{\sigma, \sigma^2, \sigma^3, \ldots\}$.

Define a map $* : G \times A \to A$ by $\sigma^i * x = \sigma^i(x)$.

We now show that G acts on A.

$$\sigma^i * (\sigma^j * x) = \sigma^i * (\sigma^j(x)) = \sigma^i(\sigma^j(x)) = (\sigma^i\sigma^j)(x) = (\sigma^i\sigma^j) * x$$

and $I * x = I(x) = x$ for all $x \in A$.

Thus, $*$ is a group action of G on A. Therefore, it partitions A into a unique set of disjoint equivalence classes called orbits.

Let $a \in A$ be any element and let $\mathcal{O}_a$ denotes the orbit of a.

Then, $\mathcal{O}_a = \{\sigma^i * a : \sigma^i \in G\} = \{\sigma^i(a) : \sigma^i \in G\}$.

Also, the stabilizer of a is given by

$$G_a = \{\sigma^i \in G : \sigma^i * a = a\} = \{\sigma^i \in G : \sigma^i(a) = a\}$$

Now G_a is a subgroup of G and G being cyclic is abelian, so G_a is normal in G.

Thus, the quotient group G/G_a exists and is of order m, where m is the least positive integer such that $\sigma^m \in G_a$.

Also, by Orbit- Stabilizer Theorem, $o(\mathcal{O}_a) = \dfrac{o(G)}{o(G_a)} = m$.

Thus, the distinct left cosets of G_a in G are

$$\sigma G_a, \sigma^2 G_a, \ldots, \sigma^{m-1} G_a, \sigma^m G_a = G_a \qquad (\text{as } \sigma^m \in G_a)$$

Again, by Orbit- Stabilizer Theorem, there exists a one–one, onto map $\varphi : \mathcal{O}_a \to G/G_a$ such that $\varphi(\sigma^i(a)) = \sigma^i G_a$. In view of this mapping the distinct members of $\mathcal{O}_a$ will be $\{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{m-1}(a)\}$.

The elements of $\mathcal{O}_a$ in this order are such that under σ, each element maps to the next element and the last element maps to the first.

This action of σ on $\mathcal{O}_a$ is expressed as a cycle permutation $(a\ \sigma(a)\ \sigma^2(a)\ \ldots\ \sigma^{m-1}(a))$.

The orbits of $\langle\sigma\rangle$, are uniquely determined by σ, therefore these cycles are unique. Also, since the orbits are disjoint, these cycles are also disjoint.

EXAMPLE:

Let $A = \{1, 2, \ldots, 10\}$ and let $\sigma \in S_{10}$ be the permutation given by

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 6 & 9 & 1 & 2 & 10 & 7 & 8 \end{bmatrix}$$

Let $G = \langle\sigma\rangle$, then as in previous theorem, we get a group action $*$ which gives a unique set of orbits.

Let us take an element 1 of A. Let $\mathcal{O}_1$ be the orbit of 1. Also, stabilizer of 1 is given by

$$G_1 = \{\sigma^i \in G : \sigma^i(1) = 1\}$$

Now, $\sigma(1) = 3$, $\sigma^2(1) = \sigma(\sigma(1)) = \sigma(3) = 4$,

$\sigma^3(1) = \sigma(\sigma^2(1)) = \sigma(4) = 6$, $\sigma^4(1) = \sigma(\sigma^3(1)) = \sigma(6) = 1$

We see that σ, σ^2, σ^3 does not belong to G_1 and $\sigma^4 \in G_1$. Thus $m = 4$, is the least positive integer such that $\sigma^4 \in G_1$.

From the above theorem, we have $o(\mathcal{O}_1) = 4$ and the elements of $\mathcal{O}_1$ are $\{1, \sigma(1), \sigma^2(1), \sigma^3(1)\} = \{1, 3, 4, 6\}$.

The corresponding cycle of σ is (1 3 4 6). Proceeding similarly with the remaining elements of A, we have

$$\sigma = (1\ 3\ 4\ 6)(2\ 5\ 9\ 7)(8\ 10)$$

Problem 10.15 Let $G = K_4$, the Klein 4–group. Label the elements e, a, b, c with the integers 1, 2, 4, 3 respectively. Prove that under the left regular action of G into S_4, the non-identity elements are mapped as follows:

$$a \to (1\ 2)(3\ 4), \quad b \to (1\ 4)(2\ 3), \quad c \to (1\ 3)(2\ 4)$$

Solution We have the permutation σ_a induced by the action of left multiplication by group element a given by

$$\sigma_a(1) = \sigma_a(e) = ae = a = 2,\ \sigma_a(2) = \sigma_a(a) = aa = e = 1,$$
$$\sigma_a(3) = \sigma_a(c) = ac = b = 4,\ \sigma_a(4) = \sigma_a(b) = ab = c = 3.$$

Thus, $\sigma_a = (1\ 2)(3\ 4)$.

Similarly, the permutation σ_b induced by the action of left multiplication by group element b given by

$$\sigma_b(1) = \sigma_b(e) = be = b = 4,\ \sigma_b(2) = \sigma_b(a) = ba = c = 3,$$
$$\sigma_b(3) = \sigma_b(c) = bc = a = 2,\ \sigma_b(4) = \sigma_b(b) = bb = e = 1.$$

Thus, $\sigma_b = (1\ 4)(2\ 3)$.

Also, the permutation σ_c induced by the action of left multiplication by group element c given by

$$\sigma_c(1) = \sigma_c(e) = ce = c = 3,\ \sigma_c(2) = \sigma_c(a) = ca = b = 4,$$
$$\sigma_c(3) = \sigma_c(c) = cc = e = 1,\ \sigma_c(4) = \sigma_c(b) = cb = a = 2.$$

Thus, $\sigma_c = (1\ 3)(2\ 4)$.

Problem 10.16 Let $G = S_3$. Label the elements I, (1 2), (2 3), (1 3), (1 2 3), (1 3 2) with the integers 1, 2, 3, 4, 5, 6 respectively. Find the image of each element of S_3 under the left regular action representation of S_3 into S_6.

Solution We have the permutation $\sigma_{(12)}$ induced by the action of left multiplication by group element (1 2) given by

$$\sigma_{(12)}(1) = \sigma_{(12)}(I) = (1\ 2)I = (1\ 2) = 2,$$
$$\sigma_{(12)}(2) = \sigma_{(12)}((1\ 2)) = (1\ 2)(1\ 2) = I = 1,$$
$$\sigma_{(12)}(3) = \sigma_{(12)}((2\ 3)) = (1\ 2)(2\ 3) = (1\ 2\ 3) = 5,$$
$$\sigma_{(12)}(4) = \sigma_{(12)}((1\ 3)) = (1\ 2)(1\ 3) = (1\ 3\ 2) = 6,$$
$$\sigma_{(12)}(5) = \sigma_{(12)}((1\ 2\ 3)) = (1\ 2)(1\ 2\ 3) = (2\ 3) = 3,$$
$$\sigma_{(12)}(6) = \sigma_{(12)}((1\ 3\ 2)) = (1\ 2)(1\ 3\ 2) = (1\ 3) = 4,$$

Thus, $(1\ 2) \mapsto (1\ 2)(3\ 5)(4\ 6)$.

Also,
$$\sigma_{(23)}(1) = \sigma_{(23)}(I) = (2\ 3)I = (2\ 3) = 3,$$
$$\sigma_{(23)}(2) = \sigma_{(23)}((1\ 2)) = (2\ 3)(1\ 2) = (1\ 3\ 2) = 6,$$
$$\sigma_{(23)}(3) = \sigma_{(23)}((2\ 3)) = (2\ 3)(2\ 3) = I = 1,$$
$$\sigma_{(23)}(4) = \sigma_{(23)}((1\ 3)) = (2\ 3)(1\ 3) = (1\ 2\ 3) = 5,$$
$$\sigma_{(23)}(5) = \sigma_{(23)}((1\ 2\ 3)) = (2\ 3)(1\ 2\ 3) = (1\ 3) = 4,$$
$$\sigma_{(23)}(6) = \sigma_{(23)}((1\ 3\ 2)) = (2\ 3)(1\ 3\ 2) = (1\ 2) = 2$$

Thus, $(2\ 3) \mapsto (1\ 3)(2\ 6)(4\ 5)$.

Similarly, it can be seen that $(1\ 3) \mapsto (1\ 4)(2\ 5)(3\ 6)$

Again,
$$\sigma_{(123)}(1) = \sigma_{(123)}(I) = (1\ 2\ 3)I = (1\ 2\ 3) = 5,$$
$$\sigma_{(123)}(2) = \sigma_{(123)}((1\ 2)) = (1\ 2\ 3)(1\ 2) = (1\ 3) = 4,$$
$$\sigma_{(123)}(3) = \sigma_{(123)}((2\ 3)) = (1\ 2\ 3)(2\ 3) = (1\ 2) = 2,$$
$$\sigma_{(123)}(4) = \sigma_{(123)}((1\ 3)) = (1\ 2\ 3)(1\ 3) = (2\ 3) = 3,$$
$$\sigma_{(123)}(5) = \sigma_{(123)}((1\ 2\ 3)) = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2) = 6,$$
$$\sigma_{(123)}(6) = \sigma_{(123)}((1\ 3\ 2)) = (1\ 2\ 3)(1\ 3\ 2) = I = 1$$

Thus, $(1\ 2\ 3) \mapsto (1\ 5\ 6)(2\ 4\ 3)$.

Similarly, $(1\ 3\ 2) \mapsto (1\ 6\ 5)(2\ 3\ 4)$.

Again,
$$\sigma_I(1) = \sigma_I(I) = II = I = 1$$
$$\sigma_I(2) = \sigma_I((1\ 2)) = I(1\ 2) = (1\ 2) = 2,$$
$$\sigma_I(3) = \sigma_I((2\ 3)) = I(2\ 3) = (2\ 3) = 3,$$
$$\sigma_I(4) = \sigma_I((1\ 3)) = I(1\ 3) = (1\ 3) = 4,$$
$$\sigma_I(5) = \sigma_I((1\ 2\ 3)) = I(1\ 2\ 3) = (1\ 2\ 3) = 5,$$
$$\sigma_I(6) = \sigma_I((1\ 3\ 2)) = I(1\ 3\ 2) = (1\ 3\ 2) = 6,$$

Thus, $I \mapsto I$.

Problem 10.17 Let $G = D_4$. Label the elements R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_D, $F_{D'}$ with the integers 1, 2, 3, 4, 5, 6, 7, 8 respectively. Find the image of each element of D_4 under the left regular action representation of D_4 into S_8.

Solution We have the permutation $\sigma_{R_{90}}$ induced by the action of left multiplication by group element R_{90} given by

$$\sigma_{R_{90}}(1) = \sigma_{R_{90}}(R_0) = R_{90}R_0 = R_{90} = 2,$$
$$\sigma_{R_{90}}(2) = \sigma_{R_{90}}(R_{90}) = R_{90}R_{90} = R_{180} = 3,$$
$$\sigma_{R_{90}}(3) = \sigma_{R_{90}}(R_{180}) = R_{90}R_{180} = R_{270} = 4,$$
$$\sigma_{R_{90}}(4) = \sigma_{R_{90}}(R_{270}) = R_{90}R_{270} = R_0 = 1,$$
$$\sigma_{R_{90}}(5) = \sigma_{R_{90}}(F_H) = R_{90}F_H = F_{D'} = 8,$$
$$\sigma_{R_{90}}(6) = \sigma_{R_{90}}(F_V) = R_{90}F_V = F_D = 7,$$
$$\sigma_{R_{90}}(7) = \sigma_{R_{90}}(F_D) = R_{90}F_D = F_H = 5,$$
$$\sigma_{R_{90}}(8) = \sigma_{R_{90}}(F_{D'}) = R_{90}F_{D'} = F_V = 6,$$

Thus, $\sigma_{R_{90}} = (1\ 2\ 3\ 4)(5\ 8\ 6\ 7)$.

Similarly, it can be seen that $\sigma_{R_0} = I$, $\sigma_{R_{180}} = (1\ 3)(2\ 4)(5\ 6)(7\ 8)$,

$$\sigma_{R_{270}} = (1\ 4\ 3\ 2)(5\ 7\ 6\ 8).$$

Again, the permutation σ_{F_H} induced by the action of left multiplication by group element F_H is given by

$$\sigma_{F_H}(1) = \sigma_{F_H}(R_0) = F_HR_0 = F_H = 5,$$
$$\sigma_{F_H}(2) = \sigma_{F_H}(R_{90}) = F_HR_{90} = F_D = 7,$$
$$\sigma_{F_H}(3) = \sigma_{F_H}(R_{180}) = F_HR_{180} = F_V = 6,$$
$$\sigma_{F_H}(4) = \sigma_{F_H}(R_{270}) = F_HR_{270} = F_{D'} = 8,$$
$$\sigma_{F_H}(5) = \sigma_{F_H}(F_H) = F_HF_H = R_0 = 1,$$
$$\sigma_{F_H}(6) = \sigma_{F_H}(F_V) = F_HF_V = R_{180} = 3,$$
$$\sigma_{F_H}(7) = \sigma_{F_H}(F_D) = F_HF_D = R_{90} = 2,$$
$$\sigma_{F_H}(8) = \sigma_{F_H}(F_{D'}) = F_HF_{D'} = R_{270} = 4$$

Thus, $\sigma_{F_H} = (1\ 5)(2\ 7)(3\ 6)(4\ 8)$.

Similarly, it can be seen that $\sigma_{F_V} = (1\ 6)(2\ 8)(3\ 5)(4\ 7)$,

$$\sigma_{F_D} = (1\ 7)(2\ 6)(3\ 8)(4\ 5),\ \sigma_{F_{D'}} = (1\ 8)(2\ 5)(3\ 7)(4\ 6),$$

Theorem 10.6: Let G be a group and H be a subgroup of G. Let G acts by left multiplication on the set A of all the left cosets of H in G. Let φ be the associated permutation representation induced by the action of G on A. Then,

(i) The action of G on A is transitive.

(ii) The stabilizer in G of $eH \in A$ is H.

(iii) The Kernel of the action is $\bigcap_{x \in G} xHx^{-1}$ and $\ker \varphi$ is the largest normal subgroup of G contained in H.

Proof: We have, $* : G \times A \to A$ be such that $g * aH = gaH$. Then G acts on A by left multiplication.

(i) Let $aH, bH \in A$ be any two members, then by taking $g = ba^{-1} \in G$, we have $g * aH = gaH = (ba^{-1})aH = bH$.

So, the action of G on A is transitive.

(ii) For any $a \in A$, $G_a = \{g \in G : g * a = a\}$.

Thus, the stabilizer of $eH = \{g \in G : g * eH = eH\}$

$$= \{g \in G : geH = eH\}$$
$$= \{g \in G : gH = H\}$$
$$= \{g \in G : g \in H\} = H$$

(iii) Let φ be the associated permutation representation, then $\varphi : G \to S_A$ is such that $\varphi(g) = \sigma_g$, where $\sigma_g : A \to A$ is given by $\sigma_g(xH) = g * xH = gxH$.

Now, $\ker\varphi = \{g \in G : \varphi(g) = I\} = \{g \in G : \sigma_g = I\}$

$$= \{g \in G : \sigma_g(xH) = I(xH) \ \forall \ x \in G\}$$
$$= \{g \in G : gxH = xH \ \forall \ x \in G\}$$
$$= \{g \in G : x^{-1}gxH = H \ \forall \ x \in G\}$$
$$= \{g \in G : x^{-1}gx \in H \ \forall \ x \in G\}$$
$$= \{g \in G : g \in xHx^{-1} \ \forall \ x \in G\}$$
$$= \bigcap_{x \in G} xHx^{-1}$$

Let $g \in$ Ker φ be any element, then $\varphi(g) = I$. This implies that $\sigma_g = I$.

Thus, $\sigma_g(aH) = I(aH) = aH$ for all $aH \in A$.

In particular, $\sigma_g(eH) = eH$ and so $geH = eH$.

Thus $gH = H$ and therefore, $g \in H$. Hence $\ker\varphi \subseteq H$.

Also, Kernels are normal subgroups, so $\ker\varphi$ is a normal subgroup of G.

We now show that $\ker\varphi$ is the largest normal subgroup of G contained in H.

Let M be any normal subgroup of G such that $M \subseteq H$. We will prove that $M \subseteq \ker\varphi$.

Let $y \in M$ be any element then to show $y \in \ker\varphi$,

i.e., $\varphi(y) = I$,

i.e., $\sigma_y = I$,

i.e., $\sigma_y(aH) = I(aH) = aH$ for all $aH \in A$.

Now, $\sigma_y(aH) = yaH = a(a^{-1}ya)H = aH$ (as $M \trianglelefteq G$, so $a^{-1}ya \in M \subseteq H$)

Thus, $y \in \ker\varphi$ and so $M \subseteq \ker\varphi$.

We now state the **Generalized Cayley's Theorem**, the proof of which follows from above theorem.

THEOREM 10.7: Let H be a subgroup of a group G and let A be the set of all left cosets of H in G. Then there is a homomorphism φ from G to S_A such that $\ker\varphi$ is the largest normal subgroup of G contained in H.

COROLLARY 10.3: Let G be a finite group of order n and p be the smallest prime such that $p|o(G)$, then any subgroup of index p is normal in G.

Proof: Let H be a subgroup of G such that $i_G(H) = p$. Let A be the set of all left cosets of H in G. Then $o(A) = p$.

Let G acts on A by left multiplication and φ be the permutation representation induced by the action of G on A such that $\ker\varphi \subseteq H$.

Let $\ker\varphi = K$ and $i_H(K) = k$. Then $o\left(\frac{G}{K}\right) = \frac{o(G)}{o(H)} \cdot \frac{o(H)}{o(K)} = pk$.

Also, since $\varphi : G \to S_A$ is a homomorphism so by first theorem of isomorphism, we have $\frac{G}{K} \cong L$, a subgroup of S_A.

Then, $o\left(\frac{G}{K}\right) = o(L)$ and $o(L) \mid o(S_A)$. Thus, $o\left(\frac{G}{K}\right) \mid o(S_A)$.

Therefore, $pk|p!$ and so $pk|p(p-1)!$

Thus, $k|(p-1)!$.

We now show that $k = 1$. Suppose on the contrary $k \neq 1$.

Let q be a prime such that $q|k$, then $q|(p-1)!$.

Thus, $q|(p-1)(p-2) \ldots 3 \cdot 2 \cdot 1$, i.e., $q|i$ for $i \leq p-1 < p$.

So, $q < p$.

Also, $o(G) = \frac{o(G)}{o(K)} o(K) = o\left(\frac{G}{K}\right) o(K) = pk \cdot o(K)$. Thus, $k|o(G)$ and so, $q|o(G)$.

But p is the smallest prime that divides $o(G)$ and $q < p$.

We thus arrive at a contradiction and so $k = 1$.

Thus, $i_H(K) = 1$ and so $o(H) = o(K)$ and hence $H = K$.

Now K being kernel of a homomorphism is normal and so H is normal in G.

We now prove the **Index Theorem** as a corollary to Generalized Cayley's theorem.

COROLLARY 10.4: Let H be a proper subgroup of a finite group G such that $i_G(H) = n$ and $o(G)$ does not divide $n!$, then G has a non-trivial normal subgroup.

Proof: By Generalized Cayley's theorem, we have the associated permutation representation φ such that $\ker\varphi$ is a normal subgroup of G contained in H.

Now, $\ker\varphi \subseteq H \subsetneq G$. Suppose $\ker\varphi = \{e\}$, then φ is one-one.

Hence $\varphi : G \to S_A$ is a one- one homomorphism and so G is isomorphic to some subgroup L of S_A.

Thus, $o(G) = o(L)$ and $o(L) | o(S_A)$.

This gives $o(G) | o(S_A) = n!$, a contradiction.

Hence $\ker\varphi \neq \{e\}$ and so $\ker\varphi$ is a non-trivial normal subgroup of G.

Remark: Index theorem can also be restated as:
If H is a proper subgroup of a finite group G such that $i_G(H) = n$ and $o(G)$ does not divide $n!$, then G is not simple.

Problem 10.18 Let H be a subgroup of G of finite index n, then prove that there is a normal subgroup K of G with $K \leq H$ and $i_G(K) \leq n!$.

Solution We have $H \leq G$ and $i_G(H) = n$. Let A be the set of all left cosets of H in G.

Let φ be the permutation representation induced by the action of G on A.

Then by first theorem of isomorphism, $\frac{G}{\ker\varphi} \cong L$, a subgroup of S_A.

Also, we have $\ker\varphi$ is a normal subgroup of G contained in H.

Let $K = \ker\varphi$, then $K \leq G$ and $K \leq H$.

Also, $o\left(\frac{G}{K}\right) = o(L)$ and $o(L) | o(S_A)$. Thus $o\left(\frac{G}{K}\right) | o(S_A) = n!$.

Therefore, $i_G(K) \leq n!$.

Problem 10.19 Let p be a prime and G be a group of order p^α for some $\alpha \in \mathbb{Z}_+$, then prove that every subgroup of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

Solution Let $o(G) = p^\alpha$, then p is the smallest prime that divides $o(G)$.

Thus, by corollary 10.3, every subgroup of index p is normal in G.

Now, suppose $o(G) = p^2$ and let $a \in G$ be such that $a \neq e$.

Then $o(a) = p$ or p^2.

If $o(a) = p^2$, then $a^{p^2} = e$ and so, $(a^p)^p = e$. Thus, $o(a^p) = p$.

Therefore, either a or a^p is an element of G of order p. This gives that G has a subgroup say H of order p.

Thus, $i_G(H) = \frac{o(G)}{o(H)} = \frac{p^2}{p} = p$ and so by first part, we have H is normal in G.

Theorem 10.8: A non-abelian finite simple group G having a subgroup H of index n is isomorphic to a subgroup of A_n.

Proof: Let G be a group with $H \leq G$ and $i_G(H) = n$. Then, by Generalized Cayley's theorem, there is a homeomorphism $\varphi : G \to S_n$ such that Kerφ is the largest normal subgroup of G contained in H.

Since G is simple, it has no non- trivial normal subgroup, thus Ker$\varphi = \{e\}$ and so φ is one- one.

Therefore, $G \cong L$, a subgroup of S_n.

Now L being a subgroup of S_n has either all members as even permutations or exactly half members as even permutations.

Suppose exactly half members of L are even permutations. Let K be the set of all even permutations of L.

Then $i_L(K) = \dfrac{o(L)}{o(K)} = 2$ and so K is normal in L.

Now since $G \cong L$, $K \trianglelefteq L$, so G has a proper normal subgroup which is not possible as G is simple.

Hence, all members of L are even permutations. Thus, L is a subgroup of S_n whose all members are even permutations.

Thus, $L \leq A_n$.

This theorem is known as **Embedding theorem.**

10.3 Group acting on themselves by Conjugation

We have already seen that if G is any group and $A = G$, then $* : G \times A \to A$ defined by $g * a = gag^{-1}$ for all $g \in G$ and $a \in A$, satisfies the axioms of group action.

This action of G on itself is called action by conjugation.

Definition 10.7: Two elements a and b of G are said to be **conjugate** in G if there exists some $g \in G$ such that $b = gag^{-1}$.

Definition 10.8: For any $a \in G$, the equivalence class of a is defined as

$$\begin{aligned} cl(a) &= \{x \in G : x \sim a\} = \{x \in G : x = g * a \text{ for some } g \in G\} \\ &= \{x \in G : x = gag^{-1} \text{ for some } g \in G\} \\ &= \{gag^{-1} : g \in G\} \end{aligned}$$

It is also called the **conjugacy class** of a. The element a is called the **representative** of the conjugacy class.

Remark: If G is abelian then $cl(a) = \{gag^{-1} : g \in G\} = \{a : g \in G\} = \{a\}$.

Definition 10.9: For any $a \in A = G$, the orbit of a in G is given by

$$\mathcal{O}_a = \{g * a : g \in G\} = \{gag^{-1} : g \in G\}$$

Thus, we say that $a, b \in G$ are conjugate if they belong to the same orbit and the orbits are nothing but the conjugacy classes.

Definition 10.10: Let G be a group and let A be a non-empty subset of G. Then

$$C_G(A) = \{g \in G : gag^{-1} = a \text{ for all } a \in A\}$$

is a subset of G, called the **centralizer of A in G.**

It is the set of all those elements of G that commute with every element of A.

Problem 10.20 Show that $C_G(A)$ is a subgroup of G.

Solution Since $ae = ea$ for all $a \in A$, so $e \in C_G(A)$ and hence $C_G(A)$ is non-empty.

Now, let $x, y \in C_G(A)$, then $xax^{-1} = a$ and $yay^{-1} = a$ for all $a \in A$.

Thus, $xax^{-1} = a \Rightarrow x^{-1}(xax^{-1})x = x^{-1}ax \Rightarrow a = x^{-1}ax$.

So, $x^{-1} \in C_G(A)$.

Also, $(xy)a(xy)^{-1} = (xy)a(y^{-1}x^{-1}) = x(yay^{-1})x^{-1} = xax^{-1} = a$.

Thus, $xy \in C_G(A)$.

Therefore, $C_G(A)$ is a subgroup of G.

Definition 10.11: Let G be a group and let A be a non-empty subset of G. Then

$$N_G(A) = \{g \in G : gAg^{-1} = A\}$$

is called the **normalizer of A in G**, where $gAg^{-1} = \{gag^{-1} : a \in A\}$.

Example:

Let G be any group and let $A = \wp(G)$, the set all subsets of G.

Define $* : G \times A \to A$ by $g * S = gSg^{-1}$.

Then,

$$g_1 * (g_2 * S) = g_1 * (g_2Sg_2^{-1}) = g_1(g_2Sg_2^{-1})g_1^{-1}$$
$$= (g_1g_2)S(g_1g_2)^{-1} = (g_1g_2) * S$$

and $e * S = eSe^{-1} = S$ for all $S \in A$.

Thus G acts on A.

Definition 10.12: Two subsets S and T of G are said to be **conjugate** in G, if there exists some $g \in G$ such that $T = gSg^{-1}$.

Remarks:

- For any subset S of G, the stabilizer of S in G is the set
$$G_S = \{g \in G : g * S = S\} = \{g \in G : gSg^{-1} = S\} = N_G(S)$$
- For any subset S of G, the orbit of S in G is the set
$$\mathcal{O}_S = \{g * S : g \in G\} = \{gSg^{-1} : g \in G\} = cl(S)$$

Problem 10.21 Let S be a subset of G and let $g \in G$, then prove that

$$gN_G(S)g^{-1} = N_G(gSg^{-1})$$

Solution We have, $x \in gN_G(S)g^{-1} \Leftrightarrow x = gyg^{-1}$ for some $y \in N_G(S)$

$\Leftrightarrow$ $g^{-1}xg = y$ for some $y \in N_G(S)$

$\Leftrightarrow$ $g^{-1}xgS(g^{-1}xg)^{-1} = S$

$\Leftrightarrow$ $g^{-1}x(gSg^{-1})x^{-1}g = S$

$\Leftrightarrow$ $x(gSg^{-1})x^{-1} = gSg^{-1}$

$\Leftrightarrow$ $x \in N_G(gSg^{-1})$

Problem 10.22 Let S be a subset of G and let $g \in G$, then prove that

$$gC_G(S)g^{-1} = C_G(gSg^{-1})$$

Solution We have, $x \in gC_G(S)g^{-1} \Leftrightarrow x = gyg^{-1}$ for some $y \in C_G(S)$

$\Leftrightarrow$ $g^{-1}xg = y$ for some $y \in C_G(S)$

$\Leftrightarrow$ $(g^{-1}xg)s(g^{-1}xg)^{-1} = s$ for all $s \in S$

$\Leftrightarrow$ $g^{-1}x(gsg^{-1})x^{-1}g = s$ for all $s \in S$

$\Leftrightarrow$ $x(gsg^{-1})x^{-1} = gsg^{-1}$ for all $gsg^{-1} \in gSg^{-1}$

$\Leftrightarrow$ $x \in C_G(gSg^{-1})$

Theorem 10.9: Let G be a group and let S be a subset of G, then the number of conjugates of S in G is the index of the normalizer of S in G.

In particular, the number of conjugates of an element x of G is the index of the centralizer of x in G.

Proof: Define a mapping $\varphi : cl(S) \to G/G_S$ by $\varphi(g * S) = gG_S$, $g \in G$. Then,

$g_1 * S = g_2 * S \Leftrightarrow {g_1}^{-1} * (g_1 * S) = {g_1}^{-1} * (g_2 * S)$

$\Leftrightarrow$ $({g_1}^{-1}g_1) * S = ({g_1}^{-1}g_2) * S$

$\Leftrightarrow$ $S = ({g_1}^{-1}g_2) * S$

$\Leftrightarrow$ ${g_1}^{-1}g_2 \in G_S$

$\Leftrightarrow$ $g_1G_S = g_2G_S$

$\Leftrightarrow$ $\varphi(g_1 * S) = \varphi(g_2 * S)$

Thus, φ is well–defined and one-one.

Also, since for any $gG_S \in G/G_S$, there exists $g * S \in cl(S)$ such that $\varphi(g * S) = gG_S$ and so φ is ontoss.

Thus φ is a bijection.

Hence $o(cl(S)) = o(G/G_S) = \dfrac{o(G)}{o(G_S)}$ = index of G_S in G = index of $N_G(S)$ in G.

Also, $o(cl(S))$ gives the number of conjugates of S in G, thus the number of conjugates of S in G is the index of the normalizer of S in G.

Further, for any $x \in G$, $N_G(x) = C_G(x)$ and so result follows.

Theorem 10.10: Let G be a finite group and let $x_1, x_2, \ldots x_r$ be the representatives of the distinct conjugacy classes of G not contained in the centre $Z(G)$ of G. Then,

$$o(G) = o(Z(G)) + \sum_{i=1}^{r} i_G(C_G(x_i))$$

This equation is known as **class equation.**

Proof: We first prove that $cl(a) = \{a\}$ if and only if $a \in Z(G)$.

Let $cl(a) = \{a\}$ and let $gag^{-1} \in cl(a)$ be any element. Then, $gag^{-1} = a$.

This gives that $ga = ag$ and so $a \in Z(G)$.

Conversely, let $a \in Z(G)$, then $ga = ag$ for all $g \in G$.

Then, $gag^{-1} = a$ for all $g \in G$ and so $cl(a) = \{a\}$.

Let $Z(G) = \{e, s_1, s_2, \ldots, s_m\}$ and let $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_r$ be the conjugacy classes of elements of G, not contained in the centre $Z(G)$ of G, with x_i as the representative of class $\mathcal{M}_i$.

Thus, the distinct conjugacy classes of G are $\{e\}, \{s_1\}, \ldots, \{s_m\}, \mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_r$.

Since the conjugacy classes partition G, we have

$$G = \{e\} \cup \{s_1\} \cup \ldots \cup \{s_m\} \cup \mathcal{M}_1 \cup \mathcal{M}_2 \cup \ldots \cup \mathcal{M}_r.$$

Therefore, $o(G) = \underbrace{1 + 1 + \ldots + 1}_{m \text{ times}} + \sum_{i=1}^{r} o(\mathcal{M}_i)$

Thus, $o(G) = o(Z(G)) + \sum_{i=1}^{r} i_G(C_G(x_i))$ (follows from theorem 10.9).

Problem 10.23 Find all the conjugacy classes and their sizes in the group Q_8. Also verify the class equation.

Solution We have $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k : i^2 = j^2 = k^2 = -1, ij = -ji = k\}$

We first show that in a group G, for any $a \in G$, $\langle a \rangle \subseteq C_G(a)$.

Let $x \in \langle a \rangle$, then $x = a^m$ for some m.

Thus, $xa = a^m a = aa^m = ax$ and so $x \in C_G(a)$.

Therefore, $\langle a \rangle \subseteq C_G(a)$.

Now, $\langle i \rangle = \{i, i^2, i^3, i^4 = 1\}$ and $\langle i \rangle \subseteq C_G(i) \subseteq G$.

Thus, $o(\langle i\rangle) | o(C_G(i)) | o(G)$, i.e., $4 | o(C_G(i)) | 8$.

This gives that $o(C_G(i)) = 4$ or 8.

Also, we have $Z(G) = \{-1, 1\}$. Now $i \notin Z(G)$ means there exist some y in G such that $iy \neq yi$.

So, $y \notin C_G(i)$ and so $C_G(i) \subsetneq G$.

Therefore, $o(C_G(i)) = 4$.

Thus, $o(cl(i)) = \dfrac{o(G)}{o(C_G(i))} = \dfrac{8}{4} = 2$

Therefore, $cl(i) = \{i, kik^{-1}\} = \{i, -kik\} = \{i, -kki\} = \{i, -i\}$.

Similarly, the other conjugate classes are $\{j, -j\}$, $\{k, -k\}$.

Also $1, -1 \in Z(G)$, so $cl(1) = \{1\}$ and $cl(-1) = \{-1\}$.

And, $o(G) = 8 = 2 + (2 + 2 + 2) = o(Z(G)) + \sum_{i=1}^{r} i_G(C_G(x_i))$.

Theorem 10.11: Let p be a prime and G be a group of prime power order p^n for some $n \geq 1$, then $Z(G) \neq \{e\}$.

Proof: If $Z(G) = G$, then $o(Z(G)) = o(G) = p^n > 1$ and so, $Z(G) \neq \{e\}$.

Now let $Z(G) \neq G$, then there exist some $x_i \in G$ such that $x_i \notin Z(G)$.

Now $x_i \notin Z(G)$ implies there exist some y in G such that $x_i y \neq y x_i$ and so $y \notin C_G(x_i)$. So, $C_G(x_i) \subsetneq G$.

Also, $o(C_G(x_i)) | o(G) = p^n$. Thus, $o(C_G(x_i)) = p^k$ for some $k < n$.

Therefore, $i_G(C_G(x_i)) = \dfrac{o(G)}{o(C_G(x_i))} = p^{n-k}$, a multiple of p.

This implies $\sum_{i=1}^{r} i_G(C_G(x_i)) = lp$, a multiple of p.

Therefore, by class equation, we have

$$o(G) = o(Z(G)) + \sum_{i=1}^{r} i_G(C_G(x_i))$$

$$\Rightarrow \quad p^n = o(Z(G)) + lp$$

$$\Rightarrow \quad o(Z(G)) = p(p^n - l)$$

Thus, $p | o(Z(G))$ and so $o(Z(G)) > 1$.

Therefore, G has a non-trivial centre.

Corollary 10.5: Let G be a group of order p^2, where p is prime, then G is abelian. Moreover, G is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Proof: Since, $o(Z(G))|o(G) = p^2$, we have $o(Z(G)) = 1$, p or p^2.

By theorem, $o(Z(G)) > 1$.

Now, if $o(Z(G)) = p^2$, then $Z(G) = G$ and so G is abelian.

If $o(Z(G)) = p$, then $o\left(\frac{G}{Z(G)}\right) = \frac{o(G)}{o(Z(G))} = p$, a prime.

Therefore, $\frac{G}{Z(G)}$ is cyclic and hence G is abelian.

Also, the partitions of 2 are 2 and 1 + 1. Thus, $G \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Problem 10.24 If the index of centre of G in G is n, then show that every conjugacy class has at most n elements.

Solution Given that $i_G(Z(G)) = n$, so, $\frac{o(G)}{o(Z(G))} = n$.

Now, let $x \in Z(G)$ then $xg = gx$ for all $g \in G$. In particular, $xa = ax$.

So $x \in C_G(a)$. Thus, $Z(G) \subseteq C_G(a)$.

This gives that $o(Z(G))|o(C_G(a))$ and so, $o(C_G(a)) = m \cdot o(Z(G))$

Therefore, $o(cl(a)) = \frac{o(G)}{o(C_G(a))} = \frac{n \cdot o(Z(G))}{m \cdot o(Z(G))} = \frac{n}{m} \leq n$.

10.4 Conjugacy in S_n

Definition 10.13: Let $\tau \in S_n$ be expressed as product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$ with $n_1 \geq n_2 \geq \ldots \geq n_r$ (including the 1 cycles), then the integers $n_1, n_2, \ldots, n_r$ are called the cycle type of τ.

Theorem 10.12: Let $\sigma, \tau \in S_n$ and suppose that σ has a cycle decomposition

$$\sigma = (x_1 x_2 \ldots x_{m_1})(y_1 y_2 \ldots y_{m_2}) \ldots (z_1 z_2 \ldots z_{m_k})$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(x_1)\ \tau(x_2) \ldots \tau(x_{m_1}))(\tau(y_1)\tau(y_2) \ldots \tau(y_{m_2})) \ldots (\tau(z_1)\tau(z_2) \ldots \tau(z_{m_k}))$$

Proof: Let $A = \{1, 2, \ldots, n\}$. Let for any $a \in A$, if $\sigma(a) = b$, then

$$\tau\sigma\tau^{-1}(\tau(a)) = \tau\sigma(\tau^{-1}(\tau(a))) = \tau\sigma(a) = \tau(\sigma(a)) = \tau(b)$$

Thus, if σ maps a to b in cyclic decomposition of σ, then $\tau(a)$ is mapped to $\tau(b)$ in the cycle decomposition of $\tau\sigma\tau^{-1}$.

Remark: We can obtain $\tau\sigma\tau^{-1}$ from σ by just replacing each entry i in the cycle decomposition of σ by the entry $\tau(i)$.

EXAMPLE:

Let $\sigma = (1\ 3\ 4)(2\ 6\ 9)(5\ 7\ 8\ 10)$ and $\tau = (1\ 3\ 7\ 5)(2\ 6\ 9\ 8)$ be any members of S_{10}. Then,

$$\tau\sigma\tau^{-1} = (\tau(1)\tau(3)\tau(4))(\tau(2)\tau(6)\tau(9))(\tau(5)\tau(7)\tau(8)\tau(10))$$
$$= (3\ 7\ 4)(6\ 9\ 8)(1\ 5\ 2\ 10)$$

PROBLEM 10.25 Let $\sigma = (1\ 2\ 3\ 4\ 5) \in S_5$. Find an element $\tau \in S_5$ such that $\tau\sigma\tau^{-1} = \sigma^2$.

SOLUTION We have $\tau\sigma\tau^{-1} = (\tau(1)\tau(2)\tau(3)\tau(4)\tau(5))$

Also, $\sigma^2 = (1\ 2\ 3\ 4\ 5)(1\ 2\ 3\ 4\ 5) = (1\ 3\ 5\ 2\ 4)$

Thus, $\tau\sigma\tau^{-1} = \sigma^2$ gives $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 5$, $\tau(4) = 2$, $\tau(5) = 4$.

Therefore, $\tau = (2\ 3\ 5\ 4)$.

PROBLEM 10.26 Let $\sigma = (1\ 2\ 3\ 4\ 5) \in S_5$. Find an element $\tau \in S_5$ such that $\tau\sigma\tau^{-1} = \sigma^{-2}$.

SOLUTION We have $\tau\sigma\tau^{-1} = (\tau(1)\tau(2)\tau(3)\tau(4)\tau(5))$

Also, $\sigma^{-2} = (\sigma^2)^{-1} = (1\ 3\ 5\ 2\ 4)^{-1} = (4\ 2\ 5\ 3\ 1)$

Thus, $\tau\sigma\tau^{-1} = \sigma^{-2}$ gives $\tau(1) = 4$, $\tau(2) = 2$, $\tau(3) = 5$, $\tau(4) = 3$, $\tau(5) = 1$.

Therefore, $\tau = (1\ 4\ 3\ 5)$.

THEOREM 10.13: Two elements in a symmetric group S_n are conjugate in S_n if and only if they have the same cycle type. Further, the number of conjugacy classes of S_n is equal to the number of partitions of n.

Proof: Let $\sigma, \tau \in S_n$ be conjugate in S_n. Then there exists a permutation ρ such that $\tau = \rho\,\sigma\rho^{-1}$.

Let $\sigma = (x_1x_2 \ldots x_{m_1})(y_1y_2 \ldots y_{m_2})\ldots(z_1z_2 \ldots z_{m_k})$. Then

$$\tau = (\rho(x_1)\ \rho(x_2) \ldots \rho(x_{m_1}))\,(\rho(y_1)\rho(y_2) \ldots \rho(y_{m_2})) \ldots (\rho(z_1)\rho(z_2) \ldots \rho(z_{m_k}))$$

Thus, σ and τ have the same cycle type.

Otherway, let $\sigma, \tau \in S_n$ have the same cycle type. We will show that σ, τ are conjugate in S_n.

Let $\sigma = (x_1x_2 \ldots x_{m_1})(y_1y_2 \ldots y_{m_2})\ldots(z_1z_2 \ldots z_{m_k})$

and $\tau = (a_1a_2 \ldots a_{m_1})(b_1b_2 \ldots b_{m_2})\ldots(c_1c_2 \ldots c_{m_k})$.

Let us choose $\rho = \begin{bmatrix} x_1 & x_2 & \ldots & x_{m_1} & \ldots & z_1 & z_1 & \ldots & z_{m_k} \\ a_1 & a_2 & \ldots & a_{m_1} & \ldots & c_1 & c_2 & \ldots & c_{m_k} \end{bmatrix}$.

Then, $\rho\,\sigma\rho^{-1} = (\rho(x_1)\rho(x_2) \ldots \rho(x_{m_1})) \ldots (\rho(z_1)\rho(z_2) \ldots \rho(z_{m_k}))$

$$= (a_1a_2 \ldots a_{m_1}) \ldots (c_1c_2 \ldots c_{m_k}) = \tau$$

Thus, σ and τ are conjugate in S_n.

We will now prove the second part of the theorem.

Let $\mathcal{A}$ denotes the set of all conjugacy classes of S_n and $\mathcal{B}$ be the set of all partitions of n.

Let $cl(\sigma) \in \mathcal{A}$ be any member.

Let $\sigma = (x_1x_2 \ldots x_{n_1})(y_1y_2 \ldots y_{n_2}) \ldots (z_1z_2 \ldots z_{n_k})$ be the representation of σ as product of disjoint cycles.

Arrange the cycles in a manner such that $n_1 \geq n_2 \geq \ldots \geq n_k$, where $\sum_{i=1}^{k} n_i = n$ and thus $\{n_1, n_2, \ldots, n_k\}$ is a partition of n and so belongs to $\mathcal{B}$.

Define a map $\theta : \mathcal{A} \to \mathcal{B}$ by $\theta(cl(\sigma)) = \{n_1, n_2, \ldots, n_k\}$.

We now show that θ is a bijection.

Let $cl(\sigma) = cl(\tau)$

$\Rightarrow$ $\sigma, \tau \in cl(\sigma)$

$\Rightarrow$ σ and τ are conjugate.

$\Rightarrow$ σ and τ have same cycle type.

$\Rightarrow$ $\tau = (a_1a_2 \ldots a_{n_1})(b_1b_2 \ldots b_{n_2}) \ldots (c_1c_2 \ldots c_{n_k})$

$\Rightarrow$ σ and τ have same corresponding partition.

$\Rightarrow$ $\theta(cl(\sigma)) = \theta(cl(\tau))$.

Thus, θ is well defined.

Now, let $cl(\sigma) \neq cl(\tau)$

$\Rightarrow$ σ and τ are not conjugate

$\Rightarrow$ σ and τ have different cycle type.

$\Rightarrow$ σ and τ have different corresponding partition.

$\Rightarrow$ $\theta(cl(\sigma)) \neq \theta(cl(\tau))$

So, θ is one–one.

Let $\{n_1, n_2, \ldots, n_k\} \in \mathcal{B}$ be any partition of n.

If we choose $\sigma = (x_1x_2 \ldots x_{n_1})(y_1y_2 \ldots y_{n_2}) \ldots (z_1z_2 \ldots z_{n_k})$, then

$\theta(cl(\sigma)) = \{n_1, n_2, \ldots, n_k\}$ and hence θ is onto.

Therefore θ is a bijection and hence $o(\mathcal{A}) = o(\mathcal{B})$.

Thus, the number of conjugacy classes of S_n is equal to the number of partitions of n.

Problem 10.27 For the symmetric group S_4, find the partitions of 4 and give the representatives of the corresponding conjugacy classes.

Solution We have

Partitions of 4	*Representatives of Conjugacy class*
4	(1 2 3 4)
3, 1	(1 2 3)(4)
2, 2	(1 2)(3 4)
2, 1, 1	(1 2)(3)(4)
1, 1, 1, 1	(1)(2)(3)(4) = I

Problem 10.28 For the symmetric group S_6, find the partitions of 6 and write the representatives of the corresponding conjugacy classes.

Solution We have

Partitions of 6	*Representatives of Conjugacy class*
6	(1 2 3 4 5 6)
5, 1	(1 2 3 4 5)(6)
4, 2	(1 2 3 4)(5 6)
4, 1, 1	(1 2 3 4)(5)(6)
3, 3	(1 2 3)(4 5 6)
3, 2, 1	(1 2 3)(4 5)(6)
3, 1, 1, 1	(1 2 3)(4)(5)(6)
2, 2, 2	(1 2)(3 4)(5 6)
2, 2, 1, 1	(1 2)(3 4)(5)(6)
2, 1, 1, 1, 1	(1 2)(3)(4)(5)(6)
1, 1, 1, 1, 1, 1	I

Problem 10.29 Let $\sigma = (1\ 2)(3\ 4\ 5)$, $\tau = (1\ 2\ 3)(4\ 5) \in S_5$. Determine whether σ and τ are conjugate. Further, if they are conjugate find an element $\rho \in S_5$ such that $\rho\sigma\rho^{-1} = \tau$.

Solution Expressing σ and τ as product of disjoint cycles with lengths in decreasing order, we have $\sigma = (3\ 4\ 5)(1\ 2)$ and $\tau = (1\ 2\ 3)(4\ 5)$.

Since σ and τ have same cycle type 2, 3, so they are conjugate.

Let $\rho \in S_5$ be such that $\rho\sigma\rho^{-1} = \tau$, then

$$(\rho(3)\rho(4)\rho(5))(\rho(1)\rho(2)) = (1\ 2\ 3)(4\ 5)$$

This gives, $\rho(3) = 1$, $\rho(4) = 2$, $\rho(5) = 3$, $\rho(1) = 4$, $\rho(2) = 5$.

Thus, $\rho = (1\ 4\ 2\ 5\ 3)$.

Problem 10.30 Let $\sigma = (1\ 5)(3\ 7\ 2)(10\ 6\ 8\ 11)$, $\tau = \sigma^3 \in S_{11}$. Determine whether σ and τ are conjugate. Further, if they are conjugate find an element $\rho \in S_5$ such that $\rho\sigma\rho^{-1} = \tau$.

Solution We have $\tau = \sigma^3 = (1\ 5)\ (10\ 11\ 8\ 6)$

Expressing σ and τ as product of disjoint cycles with lengths in decreasing order, we have $\sigma = (10\ 6\ 8\ 11)(3\ 7\ 2)(1\ 5)(4)(9)$ and $\tau = (10\ 11\ 8\ 6)(1\ 5)(2)(3)(4)(7)(9)$.

Since σ and τ have different cycle type, so they are not conjugate.

Problem 10.31 Find a representative of each conjugacy class of elements of order 4 in S_{12}.

Solution We know the order of an element in S_n, when expressed as product of disjoint cycles, is the least common multiple of the lengths of the cycles.

Now, in S_{12}, for order to be 4, the lengths must be such that their lcm is 4 and their sum is 12. Thus, we have

Class Type	*Representative of Class*
4, 4, 4	(1 2 3 4)(5 6 7 8)(9 10 11 12)
4, 4, 2, 2	(1 2 3 4)(5 6 7 8)(9 10)(11 12)
4, 2, 2, 2, 2	(1 2 3 4)(5 6)(7 8)(9 10)(11 12)
4, 4, 2, 1, 1	(1 2 3 4)(5 6 7 8)(9 10)(11)(12)
4, 4, 1, 1, 1, 1	(1 2 3 4)(5 6 7 8)(9)(10)(11)(12)
4, 2, 2, 1, 1, 1, 1	(1 2 3 4)(5 6)(7 8)(9)(10)(11)(12)
4, 2, 1, 1, 1, 1, 1, 1	(1 2 3 4)(5 6)(7)(8)(9)(10)(11)(12)
4, 2, 2, 2, 1, 1	(1 2 3 4)(5 6)(7 8)(9 10)(11)(12)
4, 1, 1, 1, 1, 1, 1, 1, 1	(1 2 3 4)(5)(6)(7)(8)(9)(10)(11)(12)

Problem 10.32 Let σ be an m – cycle in S_n. Prove that $o(C_{S_n}(\sigma)) = m(n-m)!$ and $C_{S_n}(\sigma) = \{\sigma^j \tau : \tau \in S_{n-m}, j = 0, 1, 2, \ldots, m-1\}$

Solution Let σ be an m–cycle. We first find the number of conjugates of σ. Now, a permutation will be conjugate to σ if it has same cycle type as σ, i.e., if it is an m–cycle.

Thus, $o(cl(\sigma))$ = number of conjugates of σ = number of m–cycles in S_n

$$= \frac{n!}{m(n-m)!}$$

Thus, $i_{S_n}(C_{S_n}(\sigma)) = o(cl(\sigma)) = \dfrac{n!}{m(n-m)!}$.

Therefore, $\dfrac{o(S_n)}{o(C_{S_n}(\sigma))} = \dfrac{n!}{m(n-m)!}$ and hence $o(C_{S_n}(\sigma)) = m(n-m)!$.

We know, $\langle a \rangle \subseteq C_G(a)$ for all $a \in G$, thus $\sigma^j \in C_{S_n}(\sigma)$ for all $j = 0, 1, 2, \ldots m-1$.

Since disjoint permutations commute, so a permutation τ disjoint with σ also belong to $C_{S_n}(\sigma)$.

Thus, $\{\sigma^j \tau : \tau \in S_{n-m}, j = 0, 1, 2, \ldots, m-1\} \subseteq C_{S_n}(\sigma)$.

Also, $(\{\sigma^j \tau : \tau \in S_{n-m}, j = 0, 1, 2, \ldots, m-1\}) = o(C_{S_n}(\sigma)) = m(n-m)!$

Therefore, $C_{S_n}(\sigma) = \{\sigma^j \tau : \tau \in S_{n-m}, j = 0, 1, 2, \ldots, m-1\}$.

Problem 10.33 Let $\sigma = (135) \in S_7$ be any element. Find the centralizer of σ in S_7. Also find $o(C_{S_7}(\sigma))$.

Solution We have $C_{S_7}(\sigma) = \{(135)^j \tau : \tau$ fixes 1, 3 and 5, $j = 0, 1, 2\}$.

Now, $\tau \in S_B$, where $B = \{2, 4, 6, 7\}$. Since $o(S_B) = 4!$, thus τ has 4! choices.

Therefore, $o(C_{S_7}(\sigma)) = 3.4! = 72$.

Exercises

1. Let $G = K_4$, the Klein 4–group. Label the elements e, a, b, c with the integers 1, 4, 2, 3 respectively. Prove that under the left regular action of G into S_4, the non-identity elements are mapped as follows:

$$a \to (14)(23), \quad b \to (12)(34), \quad c \to (13)(24)$$

2. Let $G = D_4$. Label the elements $R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_D, F_{D'}$ with the integers 1, 3, 5, 7, 2, 4, 6, 8 respectively. Find the image of each element of D_4 under the left regular action representation of D_4 into S_8.

3. Find all conjugacy classes and their sizes in D_4.

4. For $n = 3, 5, 7$ make lists of partitions of n and give the representatives of corresponding conjugacy classes.

5. Let $\sigma = (1\ 5)(3\ 7\ 2)(10\ 6\ 8\ 11)$, $\tau = (3\ 7\ 5\ 10)(4\ 9)(13\ 11\ 12) \in S_{13}$. Determine whether σ and τ are conjugate. Further, if they are conjugate find an element $\rho \in S_5$ such that $\rho\sigma\rho^{-1} = \tau$.

6. Let $\sigma = (1\ 2\ 3\ 4\ 5) \in S_5$. Find an element $\tau \in S_5$ such that $\tau\sigma\tau^{-1} = \sigma^{-1}$.

7. Find a representative of each conjugacy class of elements of order 4 in S_8.

8. Find the centralizer of each element of D_4, Q_8 and S_3.

9. Let $A = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ and let $G = S_3$, find the normalizer of A in G.

10. Prove that $o(C_{S_7}(1\ 2)(3\ 4)) = 8(n-4)!$ for all $n \geq 4$. Determine the centralizer explicitly.

Hints to Selected Problems

1. Proceed as in problem 10.15.

2. Proceed as in problem 10.17.

5. σ and τ are conjugate. $\rho = (1\ 4)(2)(3\ 13\ 12\ 8\ 5\ 9\ 6\ 7\ 11\ 10)$.

6. $\tau = (1\ 5)(2\ 4)(3)$.

❑❑❑

Check for updates

11

Sylow Theorems

Learning Objectives

- Sylow Subgroups
- Simple Groups

The Sylow theorems are an ensemble of results in the theory of finite groups. The common thread linking this chapter's theorems is that they determine group structure based on group order. They are results that are absolutely central to group theory, and they also serve as a partial converse to Lagrange's Theorem: 'partial' because it guarantees the existence of a subgroup only if its order is prime. They are named in honour of **P. Ludwig Sylow**†, who published these theorems in the year 1872.

11.1 *p*–Groups and Sylow *p*–subgroups

Definition 11.1: Let G be a group and let p be a prime. If $o(G) = p^n$ for some $n \geq 1$, then G is called a ***p*–group**. Subgroups of G which are p–groups are called ***p*-subgroups**.

Example:

1. Consider the group $\mathbb{Z}_9$. We have $o(\mathbb{Z}_9) = 9 = 3^2$. So $\mathbb{Z}_9$ is a 3–group.
2. Consider the group $U(32)$. Then, $o(U(32)) = 16 = 2^4$. Thus, $U(32)$ is a 2–group.

Definition 11.2: Let G be a group of order $p^n m$ where p is a prime that does not divide m, then a subgroup of order p^n is called a **Sylow *p*-subgroup** of G. The

† Peter Ludwig Mejdell Sylow was a Norwegian mathematician who was awarded an honorary doctorate from the University of Copenhagen, and went on to be appointed as an editor for Acta Mathematica.

© The Author(s) 2023

D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6_11

set of all Sylow p-subgroups of G is denoted by $\mathrm{Syl}_p(G)$ and the number of these Sylow p-subgroups of G is denoted by n_p.

We now prove the **Sylow's First theorem** which is a partial converse of Lagrange's theorem.

Theorem 11.1: Let G be a group. Let p be a prime such that p^m divides the order of G. Then G has a subgroup of order p^m.

Proof: Let $o(G) = n$. We prove the result by induction on n.

If $n = 1$, then $G = \{e\}$. In this case G is a subgroup of itself of order $1 = p^0$.

So, the result is true for $n = 1$.

Assume that result holds for all groups of order less than n.

We have $p^m | o(G)$.

Let H be a proper subgroup of G. Then two cases arise:

Case I: If $p^m | o(H)$, then by induction hypothesis H has a subgroup K of order p^m. Also K being a subgroup of H is also a subgroup of G.

So, the result holds in this case.

Case II: If $p^m \nmid o(H)$.

By class equation,

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(C_G(a))}$$

Since $a \notin Z(G)$, we have $C_G(a) \neq G$, so $p^m \nmid o(C_G(a))$.

Also, $p^m | o(G)$ implies $p^m \mid \frac{o(G)}{o(C_G(a))} . o(C_G(a))$.

Thus, $p \mid \frac{o(G)}{o(C_G(a))}$ for all $a \notin Z(G)$ (as $p^m \nmid o(C_G(a))$).

This gives that $p \mid \sum_{a \notin Z(G)} \frac{o(G)}{o(C_G(a))}$.

Then, $p \mid o(G) - \sum_{a \notin Z(G)} \frac{o(G)}{o(C_G(a))} = o(Z(G))$

Thus, by Cauchy's theorem, there exists some $x \in Z(G)$ such that $o(x) = p$.

Let $K = \langle x \rangle$ then K is a subgroup of $Z(G)$ of order p.

Thus, K is normal in G.

Then, $o(G/K) = \frac{o(G)}{o(K)} = p^{m-1} < o(G)$.

Also, $p^m \mid o(G) = \frac{o(G)}{o(K)} . o(K) = o(G/K) . o(K)$.

Since $p^m \nmid o(K)$, so $p^m | o(G/K)$.

Thus, $p^{m-1} | p^m | o(G/K)$. So by induction hypothesis, there exists a subgroup L/K of G/K such that $o(L/K) = p^{m-1}$.

Here L is a subgroup of G such that $o(L) = \frac{o(L)}{o(K)}. o(K) = p$.

Thus, we have found a subgroup L of G such that $o(L) = p^m$.

Hence the result is true in this case also.

Therefore, by induction the result holds.

Corollary 11.1: Let G be a finite group. Let p be a prime such that $p^m | o(G)$ and $p^{m+1} \nmid o(G)$ Then G has a subgroup of order p^m.

Remarks:

- This subgroup of G of order p^m is called a Sylow p-subgroup of G.
- Sylow's first theorem can also be restated as:
  Let G be a group of order $p^m \cdot k$, where p is a prime not dividing k. Then G has a subgroup of order p^m.

Theorem 11.2: Let H and K be subgroups of a group G. Let $a, b \in G$. Then the relation ~ on G defined by $a \sim b$ if and only if there exists $h \in H$, $k \in K$ such that $a = hbk$ is an equivalence relation.

Proof:

Reflexive: Since $a = eae$ for $e \in H$, $e \in K$, so $a \sim a$.

Symmetric: Let $a \sim b$, then $a = hbk$ for some $h \in H$, $k \in K$.

Now, $a = hbk$ implies $b = h^{-1}ak^{-1}$, where $h^{-1} \in H$, $k^{-1} \in K$.

Thus, $b \sim a$.

Transitive: Let $a \sim b$ and $b \sim c$. Then $a = h_1bk_1$ and $b = h_2ck_2$ for some h_1, $h_2 \in H$, $k_1, k_2 \in K$.

Thus, $a = h_1bk_1 = h_1h_2ck_2k_1 = hck$, where $h = h_1h_2 \in H$, $k = k_2k_1 \in K$.

So, $a \sim c$. Thus ~ is an equivalence relation on G.

This equivalence relation partitions G into equivalence classes given by

$$\begin{aligned} cl(a) &= \{x \in G : a \sim x\} \\ &= \{x \in G : x = hak \text{ for some } h \in H, k \in K\} \\ &= HaK \end{aligned}$$

The set HaK is called a **double coset** of H and K in G.

Also, $G = \bigcup_{a \in G} HaK$, as union of disjoint equivalence classes.

Theorem 11.3: Let H and K be subgroups of a finite group G, then $o(HaK) = \frac{o(H)o(K)}{o(H \cap aKa^{-1})}$, $a \in G$.

Proof: Define a map $\varphi : HaK \to HaKa^{-1}$ by $\varphi(hak) = haka^{-1}$, for $h \in H, k \in K$.

Then, $hak = h'ak' \Rightarrow haka^{-1} = h'ak'a^{-1} \Rightarrow \varphi(hak) = \varphi(h'ak')$.

So, φ is well defined.

Also, $\varphi(hak) = \varphi(h'ak') \Rightarrow haka^{-1} = h'ak'a^{-1} \Rightarrow hak = h'ak'$.

So, φ is one-one.

Again φ is onto as for any $haka^{-1} \in HaKa^{-1}$, the element $hak \in HaK$ such that $\varphi(hak) = haka^{-1}$.

Thus φ is a bijection.

Hence $o(HaK) = o(HaKa^{-1}) = \dfrac{o(H)o(aKa^{-1})}{o(H \cap aKa^{-1})} = \dfrac{o(H)o(K)}{o(H \cap aKa^{-1})}$.

We now prove the **Sylow's Second Theorem.**

Theorem 11.4: Any two Sylow p–subgroups of a finite group G are conjugate in G.

Proof: Let H and K be two Sylow p–subgroups of a finite group G.

Then, $o(H) = o(K) = p^m$ where $p^m | o(G)$ and $p^{m+1} \nmid o(G)$.

We need to prove that H and K are conjugate in G i.e., we need to show that $H = gKg^{-1}$ for some $g \in G$.

Suppose on contrary, $H \neq gKg^{-1}$ for all $g \in G$.

Then, $H \cap aKa^{-1}$ is a subgroup of H and so by Lagrange's theorem, $o(H \cap aKa^{-1}) = p^t$ for some $t \leq m$.

Since G can be expressed as the union of disjoint double cosets and G is finite, we have

$$o(G) = \sum_{a \in G} o(HaK)$$

Also, $o(HaK) = \dfrac{o(H)o(K)}{o(H \cap aKa^{-1})} = \dfrac{p^m p^m}{p^t} = p^{2m-t} = p^{m+1}(p^{m-t-1})$

Thus, $p^{m+1} | o(Hak)$ for all $a \in G$.

Therefore, $p^{m+1} \mid \sum_{a \in G} o(Hak) = o(G)$, which is a contradiction.

Thus, H and K are conjugate in G.

Corollary 11.2: Let N be a Sylow p-subgroup of G. Then N is a unique Sylow p-subgroup of G if and only if N is normal in G.

Proof: Let N be a unique Sylow p-subgroup of G and let $o(N) = p^m$ where $p^m | o(G)$ and $p^{m+1} \nmid o(G)$.

Let $x \in G$ be any element, then xNx^{-1} is also a subgroup of G with

$$o(xNx^{-1}) = o(N) = p^m$$

Thus, xNx^{-1} is a subgroup of G with $o(xNx^{-1}) = p^m$ such that $p^m | o(G)$ and $p^{m+1} \nmid o(G)$.

Therefore, xNx^{-1} is a Sylow p-subgroup of G.

But N is unique Sylow p-subgroup of G, so $xNx^{-1} = N$ for all $x \in G$.

Thus, N is normal in G.

Conversely, let N be a Sylow p-subgroup of G such that N is normal in G.

Let M be any other Sylow p-subgroup of G, then M and N are conjugate in G.

This gives $M = xNx^{-1}$ for some $x \in G$.

Since N is normal in G, we have $xNx^{-1} = N$ for all $x \in G$.

Therefore, $M = N$.

Hence N is a unique Sylow p-subgroup of G.

Theorem 11.5: If S is any Sylow p–subgroup of G then number of Sylow p–subgroups of G is equal to index of $N_G(S)$ in G.

Proof: We have from Theorem 10.9,

$$o(cl(S)) = o(G / G_S) = \frac{o(G)}{o(G_S)} = \frac{o(G)}{o(N_G(S))} = \text{index of } N_G(S) \text{ in } G.$$

where $cl(S) = \{P : P \leq G, P = gSg^{-1}, g \in G\}$ = set of all Sylow p–subgroups of G.

Thus, the number of Sylow p–subgroups of G is equal to index of $N_G(S)$ in G.

The next theorem known as **Sylow's third theorem** gives us a way to determine the number of Sylow subgroups a group has.

Theorem 11.6: Let G be a finite group. The number of Sylow p–subgroups of G is of the form $1 + kp$, where $1 + kp | o(G)$ and $k \geq 0$.

Proof: Let P be a Sylow p–subgroup of G. Let $o(P) = p^m$.

Then, $p^m | o(G)$ and $p^{m+1} \nmid o(G)$.

Expressing G as union of double cosets by letting $H = K = P$, we have

$$G = \bigcup_{a \in G} PaP = \bigcup_{a \in N_G(P)} PaP \bigcup_{a \notin N_G(P)} PaP$$

Thus, $o(G) = \sum_{a \in G} o(PaP) = \sum_{a \in N_G(P)} o(PaP) + \sum_{a \notin N_G(P)} o(PaP)$.

Now, $a \in N_G(P) \Rightarrow P = aPa^{-1} \Rightarrow Pa = aP \Rightarrow PPa = PaP \Rightarrow Pa = PaP$.

Thus, $\bigcup_{a \in N_G(P)} PaP = \bigcup_{a \in N_G(P)} Pa = N_G(P)$ as $P \leq N_G(P)$.

Hence, $\sum_{a \in N_G(P)} o(PaP) = o(N_G(P))$

Again, $a \notin N_G(P) \Rightarrow P \neq aPa^{-1}$

Then, $P \cap aPa^{-1}$ is a subgroup of P and so by Lagrange's theorem, $o(P \cap aPa^{-1}) = p^t$ for some $t \leq m$.

Thus, $o(PaP) = \dfrac{o(P)o(P)}{o(P \cap aPa^{-1})} = \dfrac{p^m p^m}{p^t} = p^{2m-t} = p^{m+1}(p^{m-t-1})$

Thus, $p^{m+1} \mid o(PaP)$ for all $a \in G$.

Therefore, $p^{m+1} \mid \sum_{a \notin N_G(P)} o(PaP)$ implying $\sum_{a \notin N_G(P)} o(PaP) = p^{m+1} \cdot l$ for some integer l.

Thus, $o(G) = o(N_G(P)) + p^{m+1} \cdot l$

This gives $\dfrac{o(G)}{o(N_G(P))} = 1 + \dfrac{p^{m+1} \cdot l}{o(N_G(P))}$.

By Lagrange's theorem, $o(N_G(P)) \mid o(G)$ so, $\dfrac{o(G)}{o(N_G(P))}$ is an integer.

Thus, $\dfrac{p^{m+1} \cdot l}{o(N_G(P))}$ must be an integer.

Now, $p^{m+1} \nmid o(G)$ and $N_G(P) \leq G$, so, $p^{m+1} \nmid o(N_G(P))$

Thus, $\dfrac{p^{m+1} \cdot l}{o(N_G(P))}$ is divisible by p.

This gives $\dfrac{p^{m+1} \cdot l}{o(N_G(P))} = kp$, for some integer k.

This implies $\dfrac{o(G)}{o(N_G(P))} = 1 + kp$.

Thus, number of Sylow p–subgroups of $G = 1 + kp$ (by theorem 11.5) and $1 + kp \mid o(G)$.

EXAMPLE:

Let $G = S_3$. We have $o(S_3) = 3! = 2^1 \cdot 3^1$.

Number of Sylow 2–subgroups of $G = 1 + 2k$, where $(1 + 2k) \mid 3$, as $1 + 2k$ and 2 are coprime.

This gives that $k = 0, 1$. Also, each Sylow 2–subgroup has order 2.

If $k = 0$, then there exist a unique and hence normal Sylow 2-subgroup, but there are three subgroups of order 2 in S_3, namely $\{I, (12)\}$, $\{I, (13)\}$, $\{I, (23)\}$.

Thus, $k = 1$ and S_3 has three Sylow 2-subgroups.

Again, Number of Sylow 3-subgroups of $G = 1 + 3k$, where $(1 + 3k) \mid 2$.

The only possibility for k is 1. Thus, there exists a unique and hence normal Sylow 3-subgroup of order 3, namely $\{I, (123), (132)\}$, which is nothing but A_3.

11.2 Simple Groups

Problem 11.1 Prove that a group of order 10 is not simple.

Solution Recall that a group is said to be simple if it has no non- trivial normal subgroups.

We have $o(G) = 10 = 2.5$.

Number of Sylow 5-subgroups of $G = 1 + 5k$, where $(1 + 5k)|10 = 2.5$.

Since $(1 + 5k)$ and 5 are coprime so, $(1 + 5k) \nmid 5$. Thus, $(1 + 5k) \mid 2$.

The only possibility is $k = 0$.

Thus, there exists a unique and hence normal Sylow 5–subgroup of order 5.

Therefore, G is not simple.

Problem 11.2 Let G be a group of order $2p$. Show that G has a normal subgroup of order p, where p is a prime.

Solution Number of Sylow p-subgroups of $G = 1 + pk$, where $(1 + pk)|2p$.

The possibilities are $(1 + pk) = 1$ or 2 or p or $2p$.

Since p is prime, $(1 + pk) \neq 2$. Also, $1 + pk$ is never a multiple of p.

Thus, the only possibility is $1 + pk = 1$.

Hence, there exist a unique and hence normal Sylow p-subgroup of order p.

Problem 11.3 Prove that a group of order 33 is cyclic.

Solution We have $o(G) = 33 = 3.11$.

Number of Sylow 3-subgroups of $G = 1 + 3k$, where $(1 + 3k)|11$.

The only possibility is $k = 0$.

Thus, there exists a unique and hence normal Sylow 3-subgroup, say H of order 3.

Now H being a group of prime order is cyclic. Let $H = \langle a \rangle$.

Then, $o(a) = o(H) = 3$.

Also, number of Sylow 11-subgroups of $G = 1 + 11k$, where $(1 + 11k)|3$.

This gives $k = 0$. So, there exists a unique and hence normal Sylow 11-subgroup, say K of order 11.

Since 11 is prime, K is cyclic. Let $K = \langle b \rangle$. Thus, $o(b) = o(K) = 11$.

Now, $H \cap K$ being a subgroup of H and K, we have $o(H \cap K)|o(H)$ and $o(H \cap K)|o(K)$. Thus, $o(H \cap K) = 1$ and so, $H \cap K = \{e\}$.

Also, since H and K are normal in G and $H \cap K = \{e\}$, we have $hk = kh$ for all $h \in H$ and $k \in K$.

In particular, $ab = ba$.

Thus, $ab = ba$ and $\gcd(o(a), o(b)) = \gcd(3, 11) = 1$.

Hence, $o(ab) = o(a)o(b) = 33 = o(G)$.

Thus, $G = \langle ab \rangle$ and so, G is cyclic.

Problem 11.4 Let G be a group of order pq where p and q are primes, $p < q$ and $p \nmid (q - 1)$, then show that G is cyclic.

Solution Number of Sylow p-subgroups of $G = 1 + pk$, where $(1 + pk) \mid q$.

This gives $1 + pk = 1$ or $1 + pk = q$.

If $1 + pk = q$, then $pk = q - 1$ and so, $p \mid (q - 1)$ which is not true.

Thus, $1 + pk = 1$, and so there exists a unique and hence normal Sylow p-subgroup, say H of order p.

Since p is prime, H is cyclic. Let $H = \langle a \rangle$. Then, $o(a) = o(H) = p$.

Similarly, number of Sylow q-subgroups of $G = 1 + qk$, where $(1 + qk) \mid p$.

This gives $1 + qk = 1$ or $1 + qk = p$.

If $1 + qk = p$, then $qk = p - 1$ and so $q \mid (p - 1)$. Thus, $q \leq p - 1 < p$, which is not true.

So, $1 + qk = 1$, and so there exists a unique and hence normal Sylow q-subgroup, say K of order q.

Since q is prime, K is cyclic. Let $K = \langle b \rangle$. Thus, $o(b) = o(K) = q$.

Now, $H \cap K$ being a subgroup of H and K, we have $o(H \cap K) \mid o(H)$ and $o(H \cap K) \mid o(K)$. Thus, $o(H \cap K) = 1$ and so, $H \cap K = \{e\}$.

Also, since H and K are normal in G and $H \cap K = \{e\}$, we have $hk = kh$ for all $h \in H$ and $k \in K$.

In particular, $ab = ba$.

Thus, $ab = ba$ and $\gcd(o(a), o(b)) = \gcd(p, q) = 1$.

This gives $o(ab) = o(a)o(b) = pq = o(G)$.

Thus, $G = \langle ab \rangle$ and so, G is cyclic.

Problem 11.5 Show that a group of order 35 is cyclic.

Solution We have $o(G) = 35 = 5.7$. Let $p = 5$ and $q = 7$, then p and q are distinct primes such that $p < q$ and $p \nmid (q - 1)$, so G is cyclic.

Problem 11.6 Show that a group of order 15 is cyclic.

Solution We have $o(G) = 15 = 3.5$. Let $p = 3$ and $q = 5$, then p and q are distinct primes such that $p < q$ and $p \nmid (q - 1)$, so G is cyclic.

Problem 11.7 Prove that a group of order 28 is not simple.

Solution Let $o(G) = 28 = 2^2 \cdot 7$. To prove that G is not simple we will show that G has a non-trivial normal subgroup.

Number of Sylow 7-subgroups of $G = 1 + 7k$, where $(1 + 7k) | 4$.

The only possibility is $k = 0$.

Thus, there exist a unique and hence normal Sylow 7-subgroup of order 7.

Since G has a non- trivial normal subgroup, it follows that G is not simple.

Problem 11.8 Let G be a group of order 28 having a normal subgroup of order 4. Prove that G is abelian.

Solution We have seen that G has unique and hence normal Sylow 7-subgroup of order 7.

Let K be the Sylow 7-subgroup of order 7. Then K being a group of prime order is cyclic and hence abelian.

Now, let H be a normal subgroup of order 4, then H is abelian.

Since H and K are normal in G, we have that HK is normal in G.

Also, $H \cap K$ is a subgroup of both H and K, so $o(H \cap K) | o(H) = 4$ and $o(H \cap K) | o(K) = 7$. Thus, $o(H \cap K) = 1$.

Then, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = \dfrac{4.7}{1} = 28 = o(G)$.

Thus, $G = HK$.

Now, since H and K are normal in G and $H \cap K = \{e\}$, we have $hk = kh$ for all h in H and k in K.

To show that G is abelian, we need to show that $ab = ba$ for all $a, b \in G$.

Let $a, b \in G = HK$. Then $a = h_1k_1$ and $b = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Therefore, $ab = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$

$= h_1(h_2k_1)k_2$ (since $hk = kh$ for all $h \in H$ and $k \in K$)

$= (h_1h_2)(k_1k_2) = (h_2h_1)(k_2k_1)$ (since H and K are abelian)

$= h_2(h_1k_2)k_1$

$= h_2(k_2h_1)k_1$ (since $hk = kh$ for all $h \in H$ and $k \in K$)

$= (h_2k_2)(h_1k_1) = ba$

This holds for all $a, b \in G$. Thus, G is abelian.

Problem 11.9 Let G be a group of order p^2q, where p and q are distinct primes. Then either Sylow p-subgroup or Sylow q-subgroup is normal in G.

Solution Given that $o(G) = p^2q$

Number of Sylow p-subgroups of $G = 1 + pk$, where $(1 + pk)|q$.

This gives $1 + pk = 1$ or $1 + pk = q$.

Case I: If $1 + pk = 1$, then there exists a unique and hence normal Sylow p-subgroup.

Case II: If $1 + pk = q$, then $pk = q - 1$, so $p|(q - 1)$.

Hence $p \leq (q - 1) < q$. Thus, there are q number of Sylow p-subgroups each having order p^2. These subgroups contain $q(p^2 - 1)$ non-identity elements of order p or p^2.

Out of cases I and II, one must hold.

Number of Sylow q-subgroups of $G = 1 + qk$, where $(1 + qk) | p^2$.

This gives $1 + qk = 1$ or $1 + qk = p$ or $1 + qk = p^2$

Case III: If $1 + qk = 1$, then there exists a unique and hence normal Sylow q-subgroup.

Case IV: If $1 + qk = p$, then $qk = p - 1$ and so $q|(p - 1)$.

Thus, $q \leq p - 1 < p$.

Case V: If $1 + qk = p^2$ then there are p^2 number of Sylow q-subgroups each of order q. So, there are $p^2(q - 1)$ non-identity elements of order q.

Out of cases III, IV and V one must hold.

Let H be a Sylow p-subgroup of G and K be a Sylow q-subgroup of G.

If case I holds then H is normal in G and we are done.

So, let case II holds, then $p < q$.

Here if case III holds, then K is normal in G and we are done.

If case IV holds, then $q < p$, which is a contradiction as $p < q$. So, $n_q \neq p$.

If case V holds then there are $p^2 (q - 1) + q(p^2 - 1) + 1$ elements in G, which is a contraction as $o(G) = p^2q$.

Thus, either Sylow p-subgroup or Sylow q-subgroup is normal in G.

Problem 11.10 Prove that a group of order 20 is not simple.

Solution We have $o(G) = 20 = 2^2 \cdot 5$. If we let $p = 2$ and $q = 5$, then either Sylow 2–subgroup or Sylow 5–subgroup is normal in G and hence G is not simple.

Problem 11.11 Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

Solution We have $o(G) = 56 = 2^3 \cdot 7$. The order of Sylow 2-subgroup is 8 and that of Sylow 7-subgroup is 7.

Number of Sylow 7-subgroups of $G = 1 + 7k$ such that $(1 + 7k) | 8$.

This gives $k = 0, 1$.

Case I: If $k = 0$ then there exists a unique and hence normal Sylow 7-subgroup of order 7.

Case II: If $k = 1$, then there are 8 Sylow 7-subgroups each of order 7.

Let H and K be two distinct Sylow 7-subgroups. Then $o(H \cap K) | o(H) = 7$.

Thus, $o(H \cap K) = 1$ or 7.

If $o(H \cap K) = 7$, then $H \cap K = H$. Similarly, we have $H \cap K = K$.

This gives that $H = K$, which is not true.

Thus, $o(H \cap K) = 1$ and so, $H \cap K = \{e\}$.

Therefore, these 8 Sylow 7-subgroups contain $8.(7 - 1) = 48$ non-identity elements of order 7.

Remaining elements of $G = 56 - 48 = 8$ forms a unique Sylow 2-subgroup of G, which will be normal.

Thus, from cases I and II, it can be seen that either Sylow 7-subgroup or Sylow 2-subgroup is normal in G.

Problem 11.12 Prove that a group of order 351 is not simple.

Solution Let G be a group of order 351. Then, $o(G) = 351 = 3^3 \cdot 13$.

The order of Sylow 3-subgroup is 27 and that of Sylow 13-subgroup is 13.

Number of Sylow 13-subgroups of $G = 1 + 13k$ such that $(1 + 13k) | 27$.

This gives $k = 0, 2$.

Case I: If $k = 0$ then there exists a unique and hence normal Sylow 13-subgroup of order 13.

Case II: If $k = 2$, then there are 27 Sylow 13-subgroups each of order 13.

Let H and K be two distinct Sylow 13-subgroups. Then $o(H \cap K) | o(H) = 13$.

Thus, $o(H \cap K) = 1$ or 13.

If $o(H \cap K) = 13$, then $H \cap K = H$. Similarly, we have $H \cap K = K$.

This gives that $H = K$, which is not true.

Thus, $o(H \cap K) = 1$ and so, $H \cap K = \{e\}$.

Therefore, these 27 Sylow 7-subgroups contain $27 \cdot (13 - 1) = 324$ non-identity elements of order 13.

Remaining elements of $G = 351 - 324 = 27$ forms a unique Sylow 3–subgroup of G, which will be normal.

Thus, from cases I and II, it can be seen that either Sylow 13-subgroup or Sylow 3-subgroup is normal in G.

Therefore G is not simple.

Problem 11.13 Prove that a group of order 105 has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

Solution We have $o(G) = 105 = 3 \cdot 5 \cdot 7$.

Number of Sylow 5-subgroups of $G = 1 + 5k$ such that $(1 + 5k) | 21$.

This gives $k = 0, 4$.

Case I: If $k = 0$, then there exists a unique and hence normal Sylow 5-subgroup of order 5.

Case II: If $k = 4$, then there are 21 Sylow 5-subgroups each of order 5.

Let H and K be two distinct Sylow 5-subgroups. Then $o(H \cap K) | o(H) = 5$.

Thus, $o(H \cap K) = 1$ or 5.

If $o(H \cap K) = 5$, then $H \cap K = H$. Similarly, we have $H \cap K = K$.

This gives that $H = K$, which is not true.

Thus, $o(H \cap K) = 1$ and so, $H \cap K = \{e\}$.

Therefore, these 21 Sylow 5-subgroups contain $21 \cdot (5 - 1) = 84$ non- identity elements of order 5.

Out of Cases I and II, one must hold.

Number of Sylow 7-subgroups of $G = 1 + 7k$ such that $(1 + 7k) | 15$.

This gives $k = 0, 2$.

Case III: If $k = 0$, then there exists a unique and hence normal Sylow 7-subgroup of order 7.

Case IV: If $k = 2$, then there are 15 Sylow 7- subgroups each of order 7.

Let P and Q be two distinct Sylow 7-subgroups. Then as seen earlier, we have $o(P \cap Q) = 1$ and so, $P \cap Q = \{e\}$.

Thus, these 15 Sylow 7-subgroups contain $15 \cdot (7 - 1) = 90$ non-identity elements of order 7.

Out of Cases III and IV, one must hold.

If cases II and IV holds together then G has more than $84 + 90 = 174$ elements, which is not true.

So, cases II and IV cannot hold together. Thus, out of cases I and III one must hold.

Therefore, either Sylow 5-subgroup or Sylow 7-subgroup is normal in G.

Let A be a Sylow 5-subgroup and B be a Sylow 7-subgroup of G. Then one of them is normal in G.

Thus, AB is a subgroup of G. Also, $o(A \cap B) | o(A) = 5$ and $o(A \cap B) | o(B) = 7$, so $o(A \cap B) = 1$.

Therefore, $o(AB) = \dfrac{o(A)o(B)}{o(A \cap B)} = \dfrac{5.7}{1} = 35$.

Now, suppose that A is normal in G and B is not normal in G. Then cases I and IV holds.

Since $o(AB) = 35$, it is cyclic and hence it has $\varphi(35) = 24$ elements of order 35.

Thus, G has more that $90 + 24 = 114$ elements, which is a contradiction.

Thus, B is normal in G.

Similarly, suppose that B is normal in G and A is not normal in G. Then cases II and III holds.

Thus, there are more than $84 + 24 = 108$ elements in G, which is again a contradiction.

Therefore, A is normal in G.

Hence both Sylow 5-subgroup and Sylow 7-subgroup are normal in G.

PROBLEM 11.14 Let G be a group of order 30. Then

(i) Either Sylow 3-subgroup or Sylow 5-subgroup is normal in G.

(ii) G has a normal subgroup of order 15.

(iii) Both Sylow 3-subgroup and Sylow 5-subgroup are normal in G.

SOLUTION We have $o(G) = 30 = 2 \cdot 3 \cdot 5$.

Number of Sylow 3-subgroups of $G = 1 + 3k$ such that $(1 + 3k) | 10$.

This gives $k = 0, 3$.

Case I: If $k = 0$, then there exists a unique and hence normal Sylow 3-subgroup of order 3.

Case II: If $k = 3$, then there are 10 Sylow 3-subgroups each of order 3.

Let H and K be two distinct Sylow 3-subgroups. Then $o(H \cap K) | o(H) = 3$.

Thus, $o(H \cap K) = 1$ or 3.

If $o(H \cap K) = 3$, then $H \cap K = H$. Similarly, we have $H \cap K = K$.

This gives that $H = K$, which is not true.

Thus, $o(H \cap K) = 1$ and so, $H \cap K = \{e\}$.

Therefore, these 10 Sylow 3-subgroups contain $10 \cdot (3 - 1) = 20$ non- identity elements of order 3.

Out of Cases I and II, one must hold.

Number of Sylow 5-subgroups of $G = 1 + 5k$ such that $(1 + 5k) | 6$.

This gives $k = 0, 1$.

Case III: If $k = 0$, then there exists a unique and hence normal Sylow 5-subgroup of order 5. Thus, there are 4 non- identity elements of order 5.

Case IV: If $k = 1$, then there are 6 Sylow 5-subgroups each of order 5.

As seen earlier, these 6 Sylow 5-subgroups contain $6 \cdot (5 - 1) = 24$ non- identity elements of order 5.

Out of Cases III and IV, one must hold.

(i) If cases II and IV holds together then G has more than $20 + 24 = 44$ elements, which is not true.

So, cases II and IV cannot hold together. Thus, out of cases I and III one must hold.

Therefore, either Sylow 3-subgroup or Sylow 5-subgroup is normal in G.

(ii) Let A be a Sylow 3-subgroup and B be a Sylow 5-subgroup of G. Then one of them is normal in G.

Thus, AB is a subgroup of G. Also, $o(A \cap B) | o(A) = 3$ and $o(A \cap B) | o(B) = 5$, so $o(A \cap B) = 1$.

Therefore, $o(AB) = o(AB) = \dfrac{o(A)o(B)}{o(A \cap B)} = \dfrac{3.5}{1} = 15$.

Since index of AB in $G = \dfrac{o(G)}{o(AB)} = 2$, we have AB is a normal subgroup of G.

(iii) Suppose that A is normal in G and B is not normal in G. Then cases I and IV holds.

Since $o(AB) = 15$, it is cyclic and hence it has $\varphi(15) = 8$ elements of order 15.

Thus, G has more that $8 + 24 = 32$ elements, which is a contradiction.

Thus, B is normal in G.

Similarly, suppose that B is normal in G and A is not normal in G. Then cases II and III holds.

Thus, there are more than $8 + 20 + 4 = 32$ elements in G, which is again a contradiction.

Therefore, A is normal in G.

Hence both Sylow 3-subgroup and Sylow 5-subgroup are normal in G.

Problem 11.15 Let G be a group of order pqr, where p, q, r are distinct primes with $p < q < r$. Prove that G has a normal Sylow subgroup for either p, q or r.

Solution Suppose that no Sylow subgroup of G is normal.

Number of Sylow p–subgroups is $1 + pk$ where $1 + pk | qr$.

This gives $1 + pk = q$ or r or qr with $q < r < qr$.

Number of Sylow q–subgroups is $1 + qk$ where $1 + qk | pr$.

Then $1 + qk = p$ or r or pr.

If $1 + qk = p$ then $qk = p - 1$ implying $q|(p - 1)$. So $q < p$, a contradiction.

Thus, $n_q = r$ or pr with $r < pr$.

Similarly, number of Sylow r–subgroups is $1 + rk$ where $1 + rk|pq$.

Then $1 + rk = p$ or q or pq.

If $1 + rk = p$ or q then $r < p$ or $r < q$, not true.

Thus, $n_r = pq$.

Now the Sylow p–subgroups give at least $q(p - 1)$ elements of order p and Sylow q–subgroups give at least $r(q - 1)$ elements of order q. Also, Sylow r–subgroups of G give at least $pq(r - 1)$ elements of order r.

Thus, $o(G) = pqr \geq q(p - 1) + r(q - 1) + pq(r - 1) + 1$

This gives $0 \geq rq - r - q + 1$.

This implies $(q - 1)(r - 1) \leq 0$, which is not true as q and r are primes.

Therefore, some Sylow subgroup of G is normal and hence G is not simple.

Problem 11.16 Prove that if G is a group of order 385, then $Z(G)$ contains a Sylow 7-subgroup of G and a Sylow 11-subgroup is normal in G.

Solution We have $o(G) = 385 = 5 \cdot 7 \cdot 11$.

Number of Sylow 7-subgroups of $G = 1 + 7k$ such that $(1 + 7k)|55$.

The only possibility is $k = 0$.

Thus, there exists a unique and hence normal Sylow 7- subgroup of order 7, say H.

Number of Sylow 11-subgroups of $G = 1 + 11k$ such that $(1 + 11k)|35$.

The only possibility is $k = 0$.

Thus, there exists a unique and hence normal Sylow 11-subgroup, say K of order 11.

Since K is normal in G, we can talk about the quotient group $\frac{G}{K}$.

Now, $o\left(\frac{G}{K}\right) = \frac{o(G)}{o(K)} = \frac{5.7.11}{11} = 35$.

Now, $\frac{G}{K}$ being a group of order 35 is cyclic and hence abelian.

Let G' be a commutator subgroup of G, then $G' \subseteq K$.

This gives that $o(G')|o(K)$. Thus, $o(G') = 1$ or 11.

If $o(G') = 1$, $G' = \{e\}$.

Let $a, b \in G$ be any elements, then $a^{-1}b^{-1}ab \in G' = \{e\}$.

Thus, $a^{-1}b^{-1}ab = e$ and so $ab = ba$.

Therefore, G is abelian and so $G = Z(G)$.

Thus, $H \subseteq G = Z(G)$. Hence $Z(G)$ contains a Sylow 7-subgroup of G.

Now, if $o(G') = 11$, then $G' = K$.

Let $h \in H$ and $g \in G$ then as H is normal in G, we have $g^{-1}hg \in H$.

This gives that $h^{-1}g^{-1}hg \in H$. Also, $h^{-1}g^{-1}hg \in G' = K$.

Thus, $h^{-1}g^{-1}hg \in H \cap K$.

Now, $o(H \cap K) | o(H) = 7$ and $o(H \cap K) | o(K) = 11$. Thus, $o(H \cap K) = 1$ and so $H \cap K = \{e\}$.

Therefore, $h^{-1}g^{-1}hg = e$ and so, $hg = gh$.

Thus, h commutes with all elements of G and so $h \in Z(G)$.

Therefore, $H \subseteq Z(G)$.

Thus, $Z(G)$ contains a Sylow 7-subgroup of G.

Problem 11.17 Prove that there is no simple group of order 280.

Solution Let $o(G) = 280 = 2^3 \cdot 5 \cdot 7$.

To show that G is not simple, we need to show that either Sylow 2–subgroup or Sylow 5–subgroup or Sylow 7- subgroup is normal in G.

Number of Sylow 5-subgroups of $G = 1 + 5k$ such that $(1 + 5k) | 56$.

This gives $k = 0, 11$.

Case I: If $k = 0$, then there exists a unique and hence normal Sylow 5-subgroup of order 5.

Case II: If $k = 11$, then there are 56 Sylow 5-subgroups each of order 5.

Let H and K be two distinct Sylow 5-subgroups. Then $o(H \cap K) | o(H) = 5$.

Thus, $o(H \cap K) = 1$ or 5.

If $o(H \cap K) = 5$, then $H \cap K = H$. Similarly, we have $H \cap K = K$.

This gives that $H = K$, which is not true.

Thus, $o(H \cap K) = 1$ and so, $H \cap K = \{e\}$.

Therefore, these 56 Sylow 5-subgroups contain $56 \cdot (5 - 1) = 224$ non-identity elements of order 5.

Number of Sylow 7-subgroups of $G = 1 + 7k$ such that $(1 + 7k) | 40$.

This gives $k = 0, 1$.

Case III: If $k = 0$, then there exists a unique and hence normal Sylow 7-subgroup of order 7.

Case IV: If $k = 1$, then there are 8 Sylow 7-subgroups each of order 7. Then as earlier these 8 Sylow 7-subgroups contain $8 \cdot (7 - 1) = 48$ non-identity elements of order 7.

If either case I or case III holds then we are done.

Suppose that cases II and IV holds. Then there are 224 + 48 = 272 elements in the Sylow 5-subgroups and Sylow 7-subgroups.

The remaining 8 elements of G must form a unique Sylow 2-subgroup of order 8. This unique Sylow 2-subgroup is normal.

Thus, G is not simple.

Problem 11.18 Prove that a group of order 12 is not simple.

Solution We have $o(G) = 12 = 2^2 \cdot 3$.

Let H be a Sylow 2–subgroup of G. Then $o(H) = 4$.

Thus, index of H in $G = \dfrac{o(G)}{o(H)} = \dfrac{12}{4} = 3$. Since, $12 \nmid 3!$, we have by index theorem that G is not simple.

Problem 11.19 Prove that there is no simple group of order 216.

Solution Let $o(G) = 216 = 2^3 \cdot 3^3$.

Number of Sylow 3-subgroups of $G = 1 + 3k$ such that $(1 + 3k) \mid 8$.

This gives $k = 0, 1$.

Case I: If $k = 0$, then there exists a unique and hence normal Sylow 3-subgroup of order 27 and we are done.

Case II: If $k = 1$, then there are 4 Sylow 3-subgroups each of order 27.

Let H be a Sylow 3-subgroup. Let $K = N_G(H)$.

Then by Sylow's third theorem, n_3 = index of K in G.

This gives 4 = index of K in G.

Since $216 \nmid (4)!$ we have that $o(G) \nmid (i_G(K))!$

Therefore, by index theorem, G is not simple.

Problem 11.20 Prove that there is no simple group of order 96.

Solution We have $o(G) = 96 = 2^5 \cdot 3$.

Number of Sylow 2-subgroups of $G = 1 + 2k$ such that $1 + 2k \mid 3$.

This gives $k = 0, 1$.

Case I: If $k = 0$ then there exists a unique and hence normal Sylow 2-subgroup and we are done.

Case II: If $k = 1$, then there are three Sylow 2–subgroups each of order 32.

Let P and Q be any two Sylow 2-subgroups of G.

Since $P \cap Q$ is a subgroup of P and Q, so $o(P \cap Q) \mid o(P) = 32$.

Thus, $o(P \cap Q) = 1, 2, 4, 8, 16, 32$.

If $o(P \cap Q) = 32$, then $P \cap Q = P$. Similarly, we have $P \cap Q = Q$.

This gives that $P = Q$, which is not true.

Thus, $o(P \cap Q) = 1, 2, 4, 8$ or 16.

Now, $o(PQ) = \dfrac{o(P)o(Q)}{o(P \cap Q)} = \dfrac{32.32}{o(P \cap Q)} = \dfrac{1024}{o(P \cap Q)}$.

If $o(P \cap Q) = 1, 2, 4, 8$ then $o(PQ) > o(G)$, which is not possible.

Thus, $o(P \cap Q) = 16$.

Since the index of $P \cap Q$ in P is 2, so $P \cap Q$ is a normal subgroup of P.

Similarly, $P \cap Q$ is a normal subgroup of Q.

This implies that $P, Q \subseteq N_G(P \cap Q)$ and so $PQ \subseteq N_G(P \cap Q)$.

But $o(PQ) = \dfrac{o(P)o(Q)}{o(P \cap Q)} = \dfrac{1024}{16} = 64$.

Thus, $o(N_G(P \cap Q)) \geq 64$.

Also, by Lagrange's theorem, $o(N_G(P \cap Q)) | o(G) = 96$.

Thus, $o(N_G(P \cap Q)) = 96 = o(G)$. Hence $N_G(P \cap Q) = G$.

Therefore $P \cap Q$ is a non-trivial normal subgroup of G and so G is not simple.

Problem 11.21 Let G be a group of order p^2q^2, where p and q are distinct primes such that $p \nmid (q^2 - 1)$ and $q \nmid (p^2 - 1)$. Show that G is abelian.

Solution Number of Sylow p-subgroups of $G = 1 + pk$, where $(1 + pk) | q^2$.

This gives $1 + pk = 1$ or $1 + pk = q$ or $1 + pk = q^2$.

If $1 + pk = q$, then $pk = q - 1$, so $p | (q - 1)$.

Hence $p | (q - 1)(q + 1)$ and so, $p | (q^2 - 1)$, not true.

Similarly, if $1 + pk = q^2$, then, $p | (q^2 - 1)$, which is again not true.

Thus, $1 + pk = 1$, then there exists a unique and hence normal Sylow p-subgroup say H of order p^2.

Thus, H is abelian.

In the same way we have number of Sylow q-subgroups of $G = 1 + qk$, where $(1 + qk) | p^2$.

This gives $1 + qk = 1, p, p^2$.

As discussed above we see that $1 + qk \neq p$ and $1 + qk \neq p^2$.

Thus, $1 + qk = 1$, then there exists a unique and hence normal Sylow q-subgroup K of order q^2.

Then K is abelian.

Since H, K are normal in G, we have HK is a subgroup of G.

Also, since $o(H \cap K) | o(H)$ and $o(H \cap K) | o(K)$ and p and q are coprime, so $o(H \cap K) = 1$ and thus $H \cap K = \{e\}$.

Now, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = \dfrac{p^2q^2}{1} = p^2q^2 = o(G)$.

Thus, $G = HK$. Also, $H \cap K = \{e\}$.

Therefore, $G = H \times K$. Since H and K are abelian so G is abelian.

Problem 11.22 Let G be a group of order 60. If G has more that one Sylow 5–subgroup, then show that G is simple.

Solution We have $o(G) = 60 = 2^2 \cdot 3 \cdot 5$.

Number of Sylow 5-subgroups of $G = 1 + 5k$ where $(1 + 5k) | 12$.

This gives $k = 0, 1$.

Since G has more than one Sylow 5-subgroup, we have $k \neq 0$.

Thus, $k = 1$ and so there are 6 Sylow 5-subgroups each of order 5.

Hence there exists $6(5 - 1) = 24$ non-identity elements of order 5.

Suppose G is not simple. Let H be a non-trivial normal subgroup of G.

By Lagrange's Theorem, $o(H) | o(G)$. Thus, the possible orders of H are 2, 3, 4, 5, 6, 10, 12, 15, 20, 30.

Case I: Let $o(H) = 5, 10, 15, 20, 30$ i.e., $5 | o(H)$ and $5^2 \nmid o(H)$, then H has a Sylow 5-subgroup say P.

Also $P \subseteq H \subseteq G$. If Q is any conjugate of P then $Q = gPg^{-1}$ for some g in G.

Now, $P \subseteq H \Rightarrow gPg^{-1} \subseteq gHg^{-1} = H$ (as H is normal in G.)

This gives that $Q \subseteq H$. Thus, all the six Sylow 5-subgroups which are conjugate to each other are contained in H.

This implies that all 24 non identity elements of order 5 belongs to H. Also $e \in H$.

Thus, $o(H) \geq 25$. So, in this case $o(H) = 30$. But a group of order 30 has a unique Sylow 5–subgroup. So, we get a contradiction.

Thus, $5 | o(H)$ does not hold.

Case II: Let $o(H) = 2, 3, 4$. Let $G' = G/H$.

Then $o(G') = \dfrac{o(G)}{o(H)} = \dfrac{60}{2,3,4} = 30, 20, 15$.

But we know that the groups of order 30, 20 and 15 have a unique and hence normal Sylow 5-subgroup.

Let K/H be a normal subgroup of G/H of order 5. Then, $o(K) = \dfrac{o(K)}{o(H)} \cdot o(H)$.

Thus, $o(K) = o(K/H) \cdot o(H) = 5 \cdot o(H)$.

This gives that $5 | o(K)$, which is not possible by case I.

Case III: If $o(H) = 6$ or 12, then H has a normal Sylow subgroup say T. Then T is also normal in G.

Since $o(H) = 6 = 2.3$ or $o(H) = 12 = 2^2 \cdot 3$, the possible order of Sylow subgroup T are 2 or 3 or 2^2.

That is $o(T) = 2$, 3 or 4, which is not possible by case II.

Thus, G is simple.

Problem 11.23 Prove that A_5 is simple.

Solution We have $o(A_5) = 60$.

Let $\sigma = (1\ 2\ 3\ 4\ 5)$ and $t = (1\ 3\ 2\ 4\ 5)$ be two 5-cycles in A_5.

Then, $\langle\sigma\rangle = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 = I\}$

$= \{(1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2), I\}$

and $\langle\tau\rangle = \{\tau, \tau^2, \tau^3, \tau^4, \tau^5 = I\}$

$= \{(1\ 3\ 2\ 4\ 5), (1\ 2\ 5\ 3\ 4), (1\ 4\ 3\ 5\ 2), (1\ 5\ 4\ 2\ 3), I\}$

are two Sylow 5-subgroups of A_5. So, by above problem, A_5 is simple.

Problem 11.24 Prove that the only non-trivial normal subgroup of S_5 is A_5.

Solution Let H be a non-trivial normal subgroup of S_5. Then $H \neq \{I\}$, $H \neq S_5$ and $H \trianglelefteq S_5$.

We need to show that $H = A_5$.

Consider the set $H \cap A_5$. We will show that $H \cap A_5$ is a normal subgroup of A_5.

We have $H \cap A_5 \subseteq A_5$. Let $x, y \in H \cap A_5$. Then, $x, y \in H$ and $x, y \in A_5$.

Since H and A_5 both are subgroups of S_5, so $xy^{-1} \in H$ and $xy^{-1} \in A_5$.

Thus, $xy^{-1} \in H \cap A_5$ and so $H \cap A_5$ is subgroup of A_5.

Now, let $x \in H \cap A_5$ and $g \in A_5$ be any elements.

Then, $x \in H$ and $x \in A_5$.

Now, $x \in A_5$, $g \in A_5$ implies $g^{-1}xg \in A_5$.

Also, $x \in H$, $g \in A_5 \subseteq S_5$ and $H \trianglelefteq S_5$ gives $g^{-1}xg \in H$.

Thus, $g^{-1}xg \in H \cap A_5$ and so $H \cap A_5$ is a normal subgroup of A_5.

Now, since A_5 is simple, we have $H \cap A_5 = \{I\}$ or $H \cap A_5 = A_5$.

If $H \cap A_5 = \{I\}$, then $o(H \cap A_5) = 1$.

Also, $H \trianglelefteq S_5$ and $A_5 \trianglelefteq S_5$, so HA_5 is a subgroup of S_5.

Thus, $o(HA_5) | o(S_5)$ and $o(HA_5) = \dfrac{o(H)o(A_5)}{o(H \cap A_5)} = o(H)o(A_5)$.

Then, $o(H)o(A_5) | o(S_5) = 2 \cdot o(A_5)$.

Therefore, $o(H) | 2$. So, $o(H) = 1$ or 2.

Since, $H \neq \{I\}$, so $o(H) \neq 1$. Thus, $o(H) = 2$.

We have that $H \trianglelefteq S_5$ and $o(H) = 2$ so, $H \subseteq Z(S_5)$ which is not possible as $Z(S_3) = \{I\}$.

Therefore, $H \cap A_5 = A_5$ and so $A_5 \subseteq H$.

Thus, $o(A_5)|o(H)|o(S_5)$, i.e., $60|o(H)|120$.

Therefore, $o(H) = 60$ as $H \neq S_5$.

Thus, $H = A_5$. Hence the only non-trivial normal subgroup of S_5 is A_5.

Problem 11.25 Show that A_5 cannot contain a subgroup of order 30, 20 or 15.

Solution We have that A_5 is a simple group. Thus, A_5 has no non-trivial normal subgroup.

Suppose K is a subgroup of A_5 of order 30, 20 or 15.

Then, $i_{A_5}(K) = \dfrac{o(A_5)}{o(K)} = \dfrac{60}{30,20,15} = 2,3,4.$

Thus, $(i_{A_5}(K))! = 2!$, $3!$ or $4! = 2$, 6 or 24 respectively.

Since $o(A_5)$ does not divide $(i_{A_5}(K))!$ Therefore by index theorem, A_5 is not simple, which is a contradiction.

Thus, A_5 cannot contain a subgroup of order 30, 20 or 15.

Theorem 11.7: For all $n \geq 5$, the alternating group A_n is simple.

Proof: The proof of the theorem is beyond the scope of this book.

Problem 11.26 Prove that A_n does not have a proper subgroup of index $< n$ for all $n \geq 5$.

Solution Suppose that H is a proper subgroup of A_n of index m such that $m < n$.

Let A be the set of all left cosets of H in A_n.

The action of A_n on A by left multiplication induces a homomorphism

$\varphi : A_n \to S_m$ such that $\ker\varphi$ is the largest normal subgroup of A_n contained in H.

Also, for $n \geq 5$, A_n is simple, so $\ker\varphi = \{e\}$ or $\ker\varphi = A_n$.

Since $\ker\varphi \subseteq H \subsetneq A_n$, so $\ker\varphi \neq A_n$.

Thus, $\ker\varphi = \{e\}$ and so φ is a one- one homomorphism.

Therefore, $A_n \cong K$ where K is a subgroup of S_m.

Then, $o(A_n) = o(K)$ and $o(K)|o(S_m)$. This gives $o(A_n)|o(S_m)$.

Thus, $\dfrac{n!}{2} | m!$ and so, $\dfrac{n!}{2} \leq m!$.

This implies $n(n-1)(n-2) \ldots (m+1) \leq 2$, which is not possible for $n \geq 5$.

Hence A_n does not have a proper subgroup of index less than n for all $n \geq 5$.

Problem 11.27 Let H be a subgroup of a finite group G such that $o(H)$ and $(i_G(H) - 1)!$ are coprime. Show that H is normal in G.

Solution Let A be the set of all left cosets of H in G. Then the action of G on A by left multiplication induces a homomorphism $\varphi : G \to S_A$ such that $\ker\varphi$ is the largest normal subgroup of G contained in H.

By first theorem of isomorphism, $\frac{G}{\ker\varphi} \cong K$, where K is some subgroup of S_A.

This gives $o\left(\frac{G}{\ker\varphi}\right) = o(K)$ and $o(K) | o(S_A)$.

Let $i_G(H) = n$, then $o(S_A) = n!$.

Thus, $o\left(\frac{G}{\ker\varphi}\right) | n!$. This implies $\frac{o(G)}{o(\ker\varphi)} | n!$.

Also, $\ker\varphi \subseteq H$, so $o(\ker\varphi) | o(H)$. Thus, $o(H) = k \cdot o(\ker\varphi)$.

Therefore, $\frac{o(G)}{o(\ker\varphi)} | n!$ implies $\frac{n \cdot k \cdot o(\ker\varphi)}{o(\ker\varphi)} | n!$.

Hence, $k | (n-1)!$. Also, $k | o(H)$.

Since $o(H)$ and $(n-1)!$ are coprime, we have $k = 1$.

Thus, $o(H) = o(\ker\varphi)$ and so, $\ker\varphi = H$.

Therefore, H is normal in G.

Exercises

1. Show that a group of order 40 is not simple.
2. Prove that a group of order 84 is not simple.
3. Prove that if G is a group of order 231 then $Z(G)$ contains a Sylow 11-subgroup of G and a Sylow 7-subgroup is normal in G.
4. Prove that a group of order 77 is cyclic.
5. Prove that a group of order 24 is not simple.
6. Prove that a group of order 21 is not simple.
7. Prove that a group of order 108 is not simple.
8. Prove that a group of order 72 is not simple.
9. Prove that a group of order 255 is not simple but is abelian.
10. Prove that a group of order 175 is abelian.

Hints to Selected Problems

1. $o(G) = 40 = 2^3 \cdot 5$. Show that Sylow 5-subgroup is unique.

3. Proceed as in problem 11.16.

4. Proceed as in problem 11.3.

7. Proceed as in problem 11.20.

9. Proceed as in problem 11.13.

❑❑❑

Index

A

Abelian group 6
Action by Conjugation 272, 291
Action by left multiplication 272
Action from right by multiplication 272
Algebraic structure 5
Alternating group 138
Automorphism 223, 226

B

Binary composition 4, 5

C

Cancellation Laws 33
Cauchy Theorem for finite abelian groups 191
Cayley Table 4, 8
Cayley's Theorem 213, 274
Center of a group 82
Centralizer of an element 84, 294
Centralizer of a subset 292
Centralizer of a subgroup 238
Characteristic subgroup 238
Class equation 294, 304
Commutative group 6
Commutator subgroup 188, 317
Commutators 188
Conjugacy class 291
Conjugate 291, 292
Conjugate of subgroup 86
Coset representative 143
Class representative 291
Cycle 124
Cyclic group 99
Cyclic subgroup 89, 102

D

Dihedral group 4, 51
Double coset 305

E

Embedding theorem 291
Euler φ-function 110
Even permutation 134, 291
External direct product 241, 255

F

Factor group 180
Faithful 276
Fermat's Little theorem 151
Finite group 6
Finite subgroup test 151
First isomorphism theorem 207
Fundamental theorem of cyclic groups 105
Fundamental theorem of finite abelian groups 258, 262
Fundamental theorem of homomorphism 207

© The Author(s) 2023
D. Khattar and N. Agrawal, *Group Theory*,
https://doi.org/10.1007/978-3-031-21307-6

G

General linear group 14
Generalized Cayley's theorem 288
Generator 99
Group action 271
Group homomorphism 195
Group of units 22
Groupoid 6

H

Heisenberg group 17

I

Identity element 5
Identity permutation 120
Improper normal subgroup 170
Index 149, 171
Index theorem 289, 323
Infinite group 6
Inner automorphism 227, 274
Integers under addition modulo n 20
Internal direct product 254, 266
Inverse 5
Inverse of a permutation 121
Isomorphism 205

K

Kernel of homomorphism 196, 276
Kernel of the action 275
Klein group 43

L

Lagrange's theorem 148
Left Coset 143
Left regular action 272

M

Monoid 6
Multiplication modulo n 20

N

Neutral element 5
Non trivial subgroups 70
Normal subgroup 169
Normalizer of subgroup 86
Normalizer of a subset 292

O

Odd permutation 134
One step subgroup test 72
Orbit 165, 277
Orbit Stabilizer theorem 165, 277
Order of a permutation 129
Order of an element 60
Order of a group 60

P

Partition 258, 297
Permutation 120
Permutation group 121
p-group 303
Product of cycles 125
Product of two subgroups 93
Proper subgroup 303
p-subgroup 303

Q

Quaternion group 10
Quotient group 180

R

Right coset 143

S

Second isomorphism theorem 208
Semigroup 6, 45

Simple group 170, 309
Special linear group 25
Stabilizer 164, 278
Subgroup 70
Sylow p – subgroup 303
Sylow's first theorem 304
Sylow's second theorem 306
Sylow's third theorem 307
Symmetric group 121

T

Third isomorphism theorem 208
Transitive 279
Translation 272
Transposition 131
Trivial action 271, 277
Trivial automorphism 223
Trivial subgroups 70
Two step subgroup test 71

❐❐❐